HERRE I EGET HUS?
ARBEIDSGIVERS ADGANG TIL Å OVERVÅKE SINE ANSATTE

Kandidatnummer: 512

Leveringsfrist: 27.04.2009

Til sammen 17.835 ord

14.07.2009

Innholdsfortegnelse

1 Innledning

1.1 Bakgrunn, tema og videre fremstilling

I ethvert arbeidsforhold er det i arbeidsgiverens interesse at arbeidstakeren skjøtter sitt arbeid. For å forsikre seg om dette ønsker arbeidsgivere ofte i størst mulig grad å føre kontroll med de ansattes arbeid. I tilfeller der en arbeidsgiver har konkret mistanke om at en arbeidstaker ikke overholder sine plikter i henhold til arbeidsavtalen, kan det være ønskelig med skjult kontroll for å få mistanken bekreftet eller avkreftet.

På den annen side kan arbeidstakere ha et velbegrunnet ønske om ikke å bli utsatt for utstrakt kontroll. Det kan føles inngripende å vite at man overvåkes, og at det man foretar seg på jobb, registreres og kontrolleres. Enn mer kan det føles som et overgrep for den ansatte å bli konfrontert med opplysninger som stammer fra overvåking arbeidstakeren ikke en gang visste om.

Ny teknologi gjør det i dag mulig å overvåke og loggføre andres handlinger i stort omfang. Dette var bakgrunnen for at Regjeringen i 2007 nedsatte en kommisjonen for å redegjøre for hvordan den enkeltes personvern kan ivaretas i et slikt samfunn.[1] Personvern-kommisjonens utredning, NOU 2009: 1 *Individ og integritet,* ble offentliggjort 13. januar 2009. I utredningen uttales det at nivået og omfanget av overvåking i arbeidslivet synes å ha økt betydelig de siste årene.[2] Videre pekes det på at det er blitt vanligere at arbeidsgivere tar i bruk ”politimetoder” for å avdekke mislighold blant egne ansatte.[3] For å ivareta hensynet til arbeidstakerne er det derfor nødvendig med regler som setter skranker for arbeidsgivernes adgang til å føre kontroll med sine arbeidstakere. Det er disse rettslige skrankene for kontrolltiltak som er tema for denne oppgaven.

---

[1] NOU 2009: 1 side 17.
[2] NOU 2009: 1 side 155.

Jeg vil først, i punkt 1.2, redegjøre for de ulike hensyn som gjør seg gjeldende ved kontrolltiltak i arbeidslivet. Som kontrolltiltak regnes her alle tiltak som skal sikre at arbeidstakerne utfører sitt arbeid slik de skal.[4] Videre vil jeg i kapittel 2 belyse rettskildebildet ved spørsmålet om adgangen til kontrolltiltak ettersom dette er noe uoversiktlig. Deretter gis det i kapittel 3 en oversikt over de generelle materielle og prosessuelle reglene som regulerer arbeidsgiveres adgang til kontrolltiltak.

To typer av kontrolltiltak som er blitt stadig mer utbredt er kameraovervåking på arbeidsplassen og tilsyn med de ansattes bruk av datautstyr. Av denne grunn vil den rettslige adgangen til disse to typetilfellene av kontrolltiltak vurderes særskilt, i henholdsvis kapittel 4 og 5. Et hovedspørsmål er her om arbeidsgiveres kontrolladgang går lenger enn ellers ved mistanke om mislighold fra arbeidstakeren. Dette spørsmålet er ifølge forarbeidene til arbeidsmiljøloven ikke fullt ut avklart i norsk rett.[5] Siden vedtagelsen av arbeidsmiljøloven i 2005 er imidlertid flere saker om slike kontrolltiltak i etterforskningsøyemed blitt avgjort av domstolene. Jeg vil derfor, i stor grad gjennom analyse av rettspraksis, belyse hvor grensene for kontrolladgangen går i slike situasjoner.

Temaet er for øvrig begrenset til forholdet mellom arbeidsgiver og arbeidstaker. Av denne grunn vil for eksempel ikke reglene om arbeidsgiveres meldeplikt til Datatilsynet etter personopplysningslovens regler bli behandlet.

---

[3] NOU 2009: 1 side 155.
[4] Jakhelln (2006) side 392.
[5] NOU 2004: 5 side 430.

1.2 Konkurrerende hensyn

Som nevnt kan en arbeidsgiver ha gode grunner for å føre kontroll med arbeidstakerne. Arbeidsgivere plikter blant annet å sørge for at det utføres systematisk helse-, miljø- og sikkerhetsarbeid på alle plan i virksomheten, jf. arbeidsmiljøloven § 3-1, jf. § 2-1. For å utføre denne plikten, må en arbeidsgiver nødvendigvis kontrollere at de ansatte overholder gitte sikkerhetsbestemmelser. For øvrig kan kontrolltiltak bidra til effektiv drift av virksomheten. Dette gjelder for eksempel ved kontroll av at arbeidstiden blir overholdt,[6] ved produksjons- og kvalitetskontroll [7] og ved kontrolltiltak iverksatt for å hindre nasking eller underslag.[8] Sikkerhetsmessige og bedriftsøkonomiske hensyn kan altså tale for en relativt vid adgang til kontrolltiltak.

Utstrakt bruk av kontrolltiltak kan imidlertid ha en negativ effekt på arbeidsmiljøet. Det kan oppfattes som mistenkeliggjørende og føles som et inngrep i den personlige integritet å bli overvåket. Kontrollvirksomheten kan føles som et signal om manglende tillit, og dette kan gi seg utslag i lavere arbeidsmoral. Slik kan kontrolltiltakene virke mot sin hensikt, ved at arbeidstakerne ikke yter mer enn det strengt nødvendige, eller endog mindre.

Det forekommer tilfeller der en arbeidsgiver har mistanke om at en eller flere ansatte ikke lojalt oppfyller sine plikter i henhold til arbeidsavtalen. Skjulte kontrolltiltak kan da være hensiktsmessige for å få mistanken bekreftet eller avkreftet. Ved for eksempel hemmelig videoovervåking kan det fastslås om en arbeidstaker underslår penger fra kassen. Og ved å sjekke en arbeidstakers e-post kan man finne ut om vedkommende lekker forretningshemmeligheter. Ved slik hemmelig kontroll gjør imidlertid personvernhensyn seg særlig gjeldende.[9] Det vil lett kunne føles krenkende å bli konfrontert med hemmelig innhentet informasjon, eksempelvis video- eller taleopptak, fotografier eller e-postutskrifter. I NOU 2009:1 *Individ og integritet* uttales det at arbeidslivet i Norge

[6] Fanebust (2002) side 120.
[7] NOU 2004: 5 side 429.
[8] Fanebust (2002) side 120.
[9] Dege (1995) side 386.

preges av et ønske om likevekt mellom partene.[10] Videre fremheves medarbeiderdeltakelse, større grad av ansvarliggjøring og personlig frihet som idealer.[11] Det pekes på at god informasjon og kommunikasjon mellom ansatte og arbeidsgivere er viktige virkemidler for å oppnå disse idealene. Hemmelig overvåking fremmer åpenbart ikke ønsket om likevekt mellom arbeidsgiver og arbeidstaker, og bidrar ikke til å oppnå de nevnte idealene. Reglene om kontrolltiltak må altså balansere virksomhetens kontrollbehov mot hensynet til arbeidstakernes personvern og de ulempene kontrollen kan ha for arbeidsmiljøet.

2 Rettslige utgangspunkter for adgangen til kontrolltiltak

2.1 Utgangspunktet - arbeidsgivers styringsrett

Et utgangspunkt, som nok også gjelder utenfor arbeidsrettens område, er at ethvert kontrolltiltak som virker inngripende overfor den enkelte, eller som begrenser den enkeltes handlefrihet, krever et rettslig grunnlag.[12]

Innen arbeidsretten er dette grunnlaget arbeidsgivers alminnelige styringsrett.[13] Styringsretten er av Høyesterett definert som en rett til å organisere, lede, kontrollere og fordele arbeidet,[14] men er ikke ubegrenset. Den begrenses av bestemmelser i lov, forskrift, tariffavtale og gjennom ulovfestede prinsipper.[15] I tillegg har det betydning hva slags arbeid det er tale om og hva som finnes rimelig i lys av samfunnsutviklingen.[16] Dette viser at arbeidsretten er et dynamisk rettsområde. Adgangen til kontrolltiltak vil altså endres i takt med samfunnsutviklingen.

---

[10] NOU 2009: 1 side 150.
[11] NOU 2009: 1 side 150.
[12] Ot.prp. nr. 49 (2004-2005) side 139.
[13] Ot.prp. nr. 49 (2004-2005) side 139.
[14] Rt. 2000 side 1602.
[15] Ot.prp. nr. 49 (2004-2005) side 139.
[16] Jf. Rt. 2000 side 1602.

2.2 Begrensninger i adgangen - rettskildebildet

2.2.1 Generelt

I NOU 2009: 1 uttaler Personvernkommisjonen at den anser det problematisk at reglene for personvern og integritetsvern i arbeidslivet er spredt over forskjellige lover og rettsområder.[17] Dette gjør det utfordrende for både arbeidsgivere og ansatte å orientere seg om reglene. Man risikerer dermed at reglene ikke overholdes, rett og slett fordi de er ukjente for dem de gjelder.[18] Utgangspunktet er som nevnt at en arbeidsgiver i tråd med styringsretten kan gjennomføre kontrolltiltak. Manglende kjennskap til reglene innebærer at partene ikke kjenner *begrensningene* i adgangen til å utøve kontroll. Dette medfører en fare for at det hovedsakelig er arbeidstakerne som blir skadelidende, ved at det gjennomføres inngripende kontrolltiltak som etter rettsordenen er forbudt. Under vil jeg redegjøre for de rettskildefaktorene som innebærer begrensninger i adgangen til å gjennomføre kontrolltiltak.

2.2.2 Arbeidsmiljøloven og arbeidsavtalen

De sentrale bestemmelsene om kontrolltiltak finnes i arbeidsmiljøloven. Loven kapittel 9 inneholder generelle materielle (§ 9-1) og prosessuelle (§ 9-2) regler for adgangen til å gjennomføre kontrolltiltak. Det er grunn til å understreke at man fritt kan avtale *begrensninger* i adgangen til kontrolltiltak i arbeidsavtalen. Reglene i arbeidsmiljøloven er preseptoriske, men bare til arbeidstakernes fordel, jf. § 1-9.

2.2.3 Personopplysningsloven – hvilke kontrolltiltak omfattes av loven?

Personopplysningsloven kan komme til anvendelse dersom et kontrolltiltak innebærer behandling av personopplysninger. Med behandling av personopplysninger menes enhver

[17] NOU 2009: 1 side 155.
[18] NOU 2009: 1 side 155.

bruk, herunder innsamling, av *"opplysninger og vurderinger som kan knyttes til en enkeltperson"*, jf. § 2 nr. 1 og 2. Et praktisk eksempel kan være at en arbeidsgiver tar en utskrift av en arbeidstakers e-post. Dette vil være innsamling av opplysninger som kan knyttes til en enkeltperson. [19]

Personopplysningsloven kommer bare til anvendelse i to tilfeller. Den gjelder for det første ved all behandling av personopplysninger når disse er ment å inngå i et personregister, jf. § 3 første ledd bokstav b. Personregistre er definert i forarbeidene som samlinger av materiale der identifiserbare enkeltpersoner kan brukes som søkenøkkel for å finne frem til opplysninger om vedkommende.[20] Hvis personopplysningene derimot systematiseres for eksempel kronologisk og således ikke kan finnes bare ved å slå opp på navn, faller de utenfor registerbegrepet.[21] Hvis en arbeidsgiver registrerer om de ansatte kommer for sent, gjelder altså personopplysningsloven dersom opplysningene lagres i arkiv etter navn, men ikke dersom de lagres etter dato.

For det andre regulerer loven all behandling av personopplysninger som skjer ved *"elektroniske hjelpemidler"*, jf. § 3 første ledd bokstav a. Dette innebærer at loven for eksempel gjelder ved innsyn i e-post og andre kontrolltiltak via PC. Forarbeidenes begrunnelse for at slik behandling omfattes av loven, er at det ved bruk av elektroniske hjelpemidler ofte vil være mulig å finne opplysningene ved å søke på navn.[22]

Dette gjenfinningskriteriet er imidlertid ikke nødvendigvis avgjørende ved vurderingen av om man står overfor *"elektroniske hjelpemidler"*. Personvernnemnda har, på bakgrunn av EU-retten, lagt til grunn at et viktig moment er hvorvidt behandlingen skjer automatisk, eller om den skjer ved intervensjon av mennesker.[23] Synspunktet har støtte i juridisk teori.[24] Personopplysningsloven § 3 første ledd implementerer nemlig EUs

---

[19] Se punkt 5.2.
[20] Ot.prp. nr. 92 (1998-1999) side 102.
[21] Ot.prp. nr. 92 (1998-1999) side 102.
[22] Ot.prp. nr. 92 (1998-1999) side 24.
[23] Personvernnemnda klagesak 2005: 1.
[24] Jakhelln/Aune (2005) side 337.

personverndirektiv art. 3 nr. 1. Men der begrepet *"by automatic means"* benyttes i art. 3 nr. 1, brukes altså uttrykket *"med elektroniske hjelpemidler"* i personopplysningsloven § 3 første ledd bokstav a. I forarbeidene finnes det ingen holdepunkter for at den norske regelen er ment å fravike direktivet. Derfor er det, som Personvernnemnda uttaler, naturlig å tolke den norske regelen i samsvar med EU-retten.

For å fastslå innholdet i direktivets regel, ser Personvernnemnda hen til hvordan den er implementert i EU-landenes nasjonale rett. Nemnda viser til at kriteriet *"by automatic means"* i finsk, svensk og tysk rett er implementert med regler der vurderingstemaet er i hvor stor grad mennesker har vært innblandet ved behandlingen av personopplysningene. Etter dette kommer nemnda til at et gjenfinningskriterium ikke kan være avgjørende for om man står overfor *"elektroniske hjelpemidler"*.[25] Denne konklusjonen må i kraft av nemndas argumentasjon antas å være uttrykk for gjeldende rett.

Synspunktet innebærer at en arbeidsgivers manuelle overvåking av ansatte, for eksempel ved lydopptaker eller håndholdt videokamera, ikke rammes av loven, selv om opptakeren og kameraet teknisk sett må karakteriseres som elektronisk.[26] Ved slik overvåkning er det menneskelige bidraget så stort at innsamlingen av opplysninger ikke kan sies å skje automatisk, og dermed heller ikke med elektroniske hjelpemidler.

2.2.4 Personopplysningsforskriften og merknader til forskriftsbestemmelsene

Justis- og politidepartementet og Fornyings- og administrasjonsdepartementet har med hjemmel i personopplysningsloven fastsatt utfyllende regler om behandlingen av personopplysninger. Disse reglene finnes i personopplysningsforskriften av 15. desember 2000 nr. 1265. De nye reglene i forskriften kapittel 9 er av særlig interesse ved kartleggingen av adgangen til kontrolltiltak. Disse trådte i kraft 1. mars 2009 og

[25] Personvernnemnda klagesak 2005: 1.
[26] Personvernnemnda klagesak 2005: 1.

regulerer arbeidsgiveres adgang til innsyn i de ansattes e-post. Arbeidsmiljøloven § 9-5 viser direkte til disse reglene.

Under arbeidet med forskriften har de to departementene utarbeidet merknader til de enkelte bestemmelsene. Disse merknadene er ikke inntatt i selve forskriften, men kan ses på som forarbeider til forskriftsbestemmelsene og er publisert på departementenes internettsider.[27] Merknadene kan leses som kommentarer til de enkelte bestemmelsene og baserer seg i hovedsak på avsagte rettsavgjørelser. For øvrig kan det settes spørsmålstegn ved merknadenes selvstendige betydning som rettskildefaktor. Sagt på en annen måte: hvor stor vekt skal det legges på det som er uttalt i merknadene? I underrettspraksis finnes eksempler på at det er lagt stor vekt på disse.[28] Det finnes imidlertid øyensynlig ikke eksempler på at Høyesterett i tvilsspørsmål har vurdert bestemmelsene i personopplysningsforskriften i lys av departementenes merknader. At forarbeider til forskrifter generelt kan utgjøre en relevant og tidvis også tungtveiende rettskildefaktor er imidlertid ikke tvilsomt.[29] Merknadene til personopplysningsforskriften er utformet systematisk og minner i formen om merknadene i odelstingsproposisjonene til formelle lover. Det antas at merknadene er gitt som supplement for å kunne holde selve forskriften kortfattet og generell. Dette kan tale for å tillegge forarbeidene vekt. Til dette kommer at merknadene er lett tilgjengelige for allmennheten på regjeringens internettsider.

2.2.5 Rettspraksis

Vilkårene i arbeidsmiljøloven § 9-1 om at et kontrolltiltak må være *"saklig"* og *"forholdsmessig"* er skjønnsmessige. Dette innebærer at lovgiver i stor grad har overlatt til domstolene å definere det nærmere innholdet i reglene. Rettspraksis er dermed en sentral

---

[27] Se http://www.regjeringen.no/nb/dep/fad/aktuelt/nyheter/2009/fra-i-dag-gjelder-de-nye-reglene-for-inn.html?id=547499 og http://www.regjeringen.no/nb/dep/jd/dok/lover_regler/reglement/2000/Forskrift-til-personopplysningsloven-personopplysningsforskriften/2.html?id=278534.

[28] Se for eksempel TOSLO-2001-12516.

[29] Se for eksempel Rt. 1974 side 1089 hvor et brev fra Fiskeridirektøren til Fiskeridepartementet om hva bestemmelsene burde gå ut på ble tillagt stor betydning. I dommen går ikke Høyesterett inn på spørsmålet om forarbeidene overhodet er en relevant rettskilde, men synes å ta dette for gitt. Se Eckhoff (2001) side 65 og Hilde Foyn Bruun (1980) side 7.

rettskilde når grensene for kontrolltiltak skal kartlegges. Også rettspraksis fra før arbeidsmiljøloven av 2005 er relevant ettersom regelen i § 9-1 er ment å kodifisere gjeldende ulovfestet rett.[30]

2.2.6 Praksis fra Datatilsynet og Personvernnemnda

Datatilsynet er et uavhengig offentlig organ som er gitt i oppgave å sørge for at reglene i personopplysningsloven overholdes, jf. personopplysningsloven § 42. Etter tradisjonell rettskildelære har slike organers praksis relativt liten rettskildemessig vekt.[31] Der et forvaltningsorgan består av fagfolk på området, vil organets avgjørelser imidlertid ofte være godt begrunnet. Gjennom sin argumentasjon kan dermed organet påvirke domstolene. Utover dette anser domstolene seg tradisjonelt ikke bundet av forvaltningspraksis. Høyesterett synes likevel å vektlegge Datatilsynets oppfatning der det oppstår tvilsspørsmål ved tolking av personopplysningsloven. I Rt. 2002 side 1500 viste Høyesteretts kjæremålsutvalg til Datatilsynets konklusjon i spørsmålet om en arbeidsgiver kunne lese de ansattes e-post. Datatilsynets konklusjon var helt kort og basert direkte på ordlyden i en bestemmelse i personopplysningsloven. Dette kan tilsi at det ikke var Datatilsynets argumentasjon det ble sett hen til, men nettopp tilsynets konklusjon. Datatilsynets tolkning av personopplysningsloven synes i praksis altså å bli tillagt en viss rettskildemessig vekt.

Personvernnemnda er klageorgan for Datatilsynets avgjørelser. Nemnda består av eksperter innen temaet personvern, og nemndas avgjørelser er ofte enda grundigere juridisk begrunnet enn tilsynets. Dette taler for at deres praksis bør tillegges ytterligere vekt i forhold til Datatilsynets.

2.2.7 Internasjonale rettskilder

I rettspraksis finnes det påfallende få henvisninger til internasjonale rettskilder i saker om kontrolltiltak. Dette betyr ikke at Norge ikke er underlagt folkerettslige forpliktelser i

[30] Ot.prp. nr. 49 (2004-2005) side 314.

forbindelse med kontrolltiltak, men kan i noen grad tyde på at det norske regelverket oppfyller forpliktelsene.

Den europeiske menneskerettskonvensjon (EMK) er gjort til norsk lov, jf. menneskerettsloven § 2. Bestemmelsene der må tolkes i samsvar med praksis fra Den europeiske menneskerettsdomstol (EMD). I art. 8 oppstilles en rett til respekt for privatlivet. Denne retten gjelder etter EMDs praksis også på arbeidsplassen.[32] I flere saker er stater dømt for å ha tillatt kontrolltiltak i arbeidslivet som etter EMDs syn krenket retten til privatliv.[33] I forarbeidene til personopplysningsloven uttales at loven oppfyller kravene som følger av EMK art. 8.[34] Selv om dette nok er riktig, er det ingen garanti mot at EMD med sin dynamiske tolkningsmetode i fremtiden kan finne at norske regler om kontrolltiltak strider mot retten til privatliv. Høyesterett har for øvrig presisert at det i første rekke er opp til EMD, ikke norske domstoler, å utvikle EMK-retten.[35]

Også EU-retten har betydning ved fastleggingen av de norske reglene om kontrolltiltak. Bestemmelsene i personopplysningsloven bygger nemlig på EUs personverndirektiv.[36] Det uttales riktignok ikke i forarbeidene at loven direkte implementerer direktivet, men etter utarbeidelsen av loven er direktivet blitt en del av EØS-avtalen.[37] Norge plikter derfor å ha regler som samsvarer med direktivet.[38] Personopplysningsloven må av denne grunn tolkes i lys av EU-retten. For øvrig er personverndirektivet et såkalt minimumsdirektiv.[39] Dette innebærer at norske regler gjerne kan statuere et strengere personvern enn det direktivet legger opp til. En forutsetning er imidlertid at de norske reglene ikke strider mot direktivet

---

[31] Eckhoff (2001) side 233.
[32] Se for eksempel sak 1992-12-16 *Niemietz mot Tyskland*.
[33] Se for eksempel sak 2007-04-03 *Copland mot Storbritannia*.
[34] NOU 1997: 19 pkt. 9.3.
[35] Rt. 2000 side 996.
[36] Ot.prp. nr. 92 (1998-1999) side 14.
[37] EØS-komiteens beslutning nr. 83/1999.
[38] EØS art. 7.
[39] Direktivets fortale avsnitt 9 og 10.

som helhet, og da særlig prinsippet om fri flyt av personopplysninger innen EU, jf. art. 1 nr. 2.[40]

3 Generelle vilkår for å gjennomføre kontrolltiltak

3.1 Innledning

Arbeidsmiljøloven og personopplysningsloven inneholder generelle regler om hva som skal til for at en arbeidsgiver kan gjennomføre kontrolltiltak overfor sine arbeidstakere. I tillegg inneholder begge lovene regler om informasjonsplikt i forbindelse med at tiltakene iverksettes. Det er ved fremstillingen av de generelle vilkårene for å gjennomføre kontrolltiltak hensiktsmessig å skille mellom de materielle (punkt 3.2) og prosessuelle (punkt 3.3) reglene som kommer til anvendelse.

3.2 Oversikt over de materielle grunnvilkårene for kontrolltiltak

3.2.1 Reglene i arbeidsmiljøloven

Innen arbeidsretten gjelder det et generelt krav til saklighet ved arbeidsgivers behandling av sine arbeidstakere.[41] Dette medfører begrensninger i en arbeidsgivers adgang til å styre virksomheten som vedkommende vil. I relasjon til kontrolltiltak er dette saklighetsprinsippet nå lovfestet. I henhold til arbeidsmiljøloven § 9-1 første ledd kan en arbeidsgiver bare iverksette kontrolltiltak overfor en arbeidstaker når tiltaket har *"saklig grunn i virksomhetens forhold"* og det ikke innebærer en *"uforholdsmessig belastning for arbeidstakeren"*.

[40] NOU 2009: 1 side 58.
[41] Se for eksempel Rt. 2001 side 418.

Saklighets- og forholdsmessighetskravet kan ikke tilsidesettes ved samtykke.[42] Dette følger av § 1-9 om at loven ikke kan fravikes til ugunst for arbeidstaker. En slik adgang ville lett kunne medført at arbeidstakeren følte seg presset til å godta kontrolltiltakene, og på denne måten gjøre vilkårene illusoriske.[43]

At tiltaket må ha saklig grunn innebærer for det første at det må foreligge et saklig formål for kontrollen, begrunnet i virksomheten som sådan.[44] Forsvaret kan således pålegge en yrkessoldat en kondisjonstest. Det samme gjelder neppe overfor en kontormedarbeider, selv om arbeidsgiveren kan ha et aldri så stort ønske om sunne og friske medarbeidere. Eksempelet illustrerer også at kravet om saklig grunn må være oppfylt overfor den enkelte arbeidstaker som berøres av kontrolltiltaket.[45] Usaklig forskjellsbehandling av arbeidstakere, eller grupper av ansatte, i forbindelse med kontrolltiltak er forbudt i samsvar med det alminnelige saklighetsprinsippet innen arbeidsretten.[46]

Videre må tiltaket for å ha saklig grunn være *"egnet til"* og *"nødvendig for å gjennomføre formålet"*.[47] Dersom formålet er å kontrollere at arbeidstakerne møter på arbeidsstedet til rett tid, vil for eksempel registrering av om vedkommendes PC er slått på, neppe være egnet fordi den ansatte kanskje gjør andre arbeidsoppgaver før vedkommende slår på PC'en. Videoovervåking av lokalet vil derimot kunne være meget godt egnet til dette formålet. På den annen side vil tradisjonell inn- og utstempling kunne være like godt egnet. Etter forarbeidene vil et moment ved nødvendighetsvurderingen være om det aktuelle formålet kan ivaretas på en annen, mindre belastende måte. [48] I eksempelet over vil videoovervåkning åpenbart oppleves som mer inngripende enn et tradisjonelt stemplingssystem. Når det ikke er nødvendig å gå så drastisk til verks for å oppnå formålet vil videoovervåkingen ikke ha saklig grunn.

---

[42] Ot.prp. nr. 49 (2004-2005) side 144.
[43] Jakhelln/Aune (2005) side 332.
[44] Ot.prp. nr. 49 (2004-2005) side 144.
[45] Ot.prp. nr. 49 (2004-2005) side 145.
[46] Jakhelln (2006) side 397.
[47] Ot.prp. nr. 49 (2004-2005) side 145.
[48] Ot.prp. nr. 49 (2004-2005) side 145.

I henhold til forarbeidene må saklig grunn foreligge på ethvert tidspunkt. [49] Dette innebærer at kontrolltiltaket må opphøre når det behovet eller formålet som begrunnet tiltaket ikke lenger gjør seg gjeldende.

I tillegg til å være saklig begrunnet, må et kontrolltiltak ikke innebære en *"uforholdsmessig belastning"* for arbeidstakeren, jf. § 9-1 første ledd. I dette ligger at det må foretas en avveining av arbeidsgiverens behov for kontrolltiltaket mot de ulempene tiltaket medfører for arbeidstakeren. Ved vurderingen av ulemper må man se samlet på summen av kontrolltiltak i virksomheten.[50] Et tiltak som isolert sett bare er til litt bry, kan være uforholdsmessig dersom det allerede foreligger en rekke byrdefulle kontrolltiltak.

For øvrig beror vurderingen i henhold til forarbeidene på tiltakets formål, varigheten, hvor ofte det gjennomføres og hvilke inngrep i arbeidstakernes personvern det vil være tale om. Videre har det betydning om arbeidsgiveren har sørget for at uvedkommende ikke får tilgang til de data som samles inn.[51] Ved vurderingen av kontrolltiltakets lovlighet etter arbeidsmiljøloven har det altså betydning hvordan innsamlede opplysninger behandles i ettertid. Dette viser at reglene i arbeidsmiljøloven og personopplysningsloven er knyttet nært sammen.

3.2.2 Reglene i personopplysningsloven

Som nevnt kommer personopplysningsloven til anvendelse ved kontrolltiltak som innebærer behandling av personopplysninger enten elektronisk eller for lagring i et personregister. I disse tilfellene må kontrolltiltakets lovlighet vurderes etter både arbeidsmiljølovens og personopplysningslovens regler.

---

[49] Ot.prp. nr. 49 (2004-2005) side 145.
[50] Ot.prp. nr. 49 (2004-2005) side 145.
[51] Ot.prp. nr. 49 (2004-2005) side 145.

Personopplysningsloven bygger på EUs personverndirektiv og prinsippet om rett til selv å bestemme over opplysninger om seg selv.[52] I henhold til personopplysningsloven § 8 første ledd trengs som utgangspunkt samtykke for at en arbeidsgiver skal kunne behandle en arbeidstakers personopplysninger. Uten slikt samtykke kan de behandles bare dersom det er fastsatt i lov, eller dersom behandlingen er nødvendig for å oppnå et formål uttømmende opplistet i § 8.

Det mest praktiske er at behandlingen er nødvendig for å ivareta en berettiget interesse, og hensynet til den registrertes personvern ikke overstiger denne interessen, jf. § 8 bokstav f. Det må altså, som etter bestemmelsen i arbeidsmiljøloven § 9-1, foretas en interesseavveining. Når det som nevnt etter arbeidsmiljøloven kreves et saklig formål og det også har betydning hvordan innsamlet data sikres, er det klart at vurderingen etter de to lover må bli ganske lik. I forarbeidene uttales det da også at det vanligvis foreligger behandlingsadgang etter personopplysningsloven dersom vilkårene etter arbeidsmiljøloven er oppfylt.[53] Synspunktet har støtte i underrettspraksis. Det finnes der eksempler på at retten har nøyd seg med én samlet vurdering av kontrolltiltaket, da på bakgrunn av arbeidsmiljøloven § 9-1 første ledd.[54]

I forarbeidene til arbeidsmiljøloven uttalte arbeidslivslovutvalget at det antagelig er en absolutt gyldighetsbetingelse at et kontrolltiltak ikke virker krenkende overfor arbeidstakeren.[55] Ordlyden i odelstingsproposisjonen er noe mer moderat. Det sies her at dersom kontrolltiltaket medfører et ikke ubetydelig inngrep i rettsgoder som personlig integritet, verdighet, privatlivets fred, legemets ukrenkelighet eller lignende, vil vilkårene for å gjennomføre kontrollen bare unntaksvis være oppfylt. [56] Hovedregelen er altså at det ikke er adgang til å gjennomføre kontrolltiltak som vil oppleves som integritetskrenkende.

[52] Se nærmere NOU 2004: 5 side 419.
[53] Ot.prp. nr. 49 (2004-2005) side 146.
[54] Se for eksempel LB-2007-121782.
[55] NOU 2004: 5 side 430.
[56] Ot.prp. nr. 49 (2004-2005) side 145.

Imidlertid uttales det også i forarbeidene at det skal mye til for at kontroll i forbindelse med konkret mistanke om mislighold vil bli ansett uforholdsmessige.[57] Det må til dette sies at et kontrolltiltak på bakgrunn av konkret mistanke typisk vil medføre et *"ikke ubetydelig inngrep"* i den personlige integritet. Når det likevel skal mye til for at slike tiltak anses uforholdsmessige, gir dette en klar indikasjon på at konkret mistanke om mislighold nettopp er en omstendighet som kan begrunne unntak fra hovedregelen om at integritetskrenkende tiltak er uforholdsmessige. Hvor grensene går i slike tilfeller vurderes i kapitlene om kameraovervåking og e-postinnsyn.

3.3 Prosessuelle vilkår for kontrolltiltak – informasjon og drøfting

3.3.1 Informasjons- og drøftingsplikten i arbeidsmiljøloven

Det følger av arbeidsmiljøloven § 9-2 første ledd at en arbeidsgiver så tidlig som mulig plikter å drøfte behov, utforming, gjennomføring og vesentlig endring av kontrolltiltak med arbeidstakernes tillitsvalgte. Representanter for de ansatte skal gis en reell mulighet til å komme med innspill og innvendinger.[58] Regelen kan sies å bidra til målet om likevekt og medarbeiderdeltakelse i arbeidslivet.[59] Likevel er det etter ordlyden kun tale om en plikt til å drøfte. I følge forarbeidene er det arbeidsgiveren som bestemmer dersom partene ikke blir enige.[60]

I tillegg til drøftingsplikten, må en arbeidsgiver før selve iverksettelsen av kontrolltiltaket gi de berørte arbeidstakerne informasjon om tiltaket, jf. § 9-2 annet ledd. Utover å angi tiltakets formål, skal arbeidsgiveren angi hvilke praktiske konsekvenser det vil medføre, herunder antatt varighet.

---

[57] Ot.prp. nr. 49 (2004-2005) side 145.
[58] NOU 2004: 5 side 435.
[59] Se punkt 1.2.
[60] NOU 2004: 5 side 435.

Et spørsmål er om hvert enkelt tilfelle av kontroll utløser en informasjonsplikt i forkant av tiltaket. Sett i lys av ønsket om likevekt mellom partene[61] og hensynet til et godt og forsvarlig arbeidsmiljø,[62] kan det hevdes at arbeidsgiveren nettopp burde gi de berørte arbeidstakerne informasjon før den enkelte kontroll. Dette synspunktet underbygges av bestemmelsen i § 4-3 første ledd, jf. § 2-1 om at arbeidsgivere skal sørge for at arbeidstakernes integritet og verdighet ivaretas.

I forarbeidene til bestemmelsen i § 9-2 er det imidlertid uttalt at det ikke er meningen at gjennomføring av den enkelte kontroll i seg selv skal utløse drøftings- og informasjonsplikt.[63] En slik plikt ville vært tungvint og lite formålstjenlig. Blir den ansatte for eksempel varslet før ransaking, vil han kunne kvitte seg med tyvegods og tiltaket ville vært lite effektivt. Reelle hensyn taler altså mot at informasjon kan kreves før hvert enkelt kontrolltiltak. Tolket i lys av forarbeidene og reelle hensyn, innebærer bestemmelsen i § 9-2 andre ledd bare at informasjon i det hele tatt blir gitt på ett eller annet tidspunkt før kontrolltiltaket iverksettes. Informasjonen kan for eksempel gis til nye ansatte ved inngåelsen av arbeidsavtalen, selv om kontrolltiltaket først iverksettes på et senere tidspunkt.

Det kan spørres om en arbeidsgiver kan vente ubegrenset lenge fra informasjon gis til tiltaket iverksettes, eller om han på noen måte må "holde informasjonen varm". I Rt. 2005 side 518 måtte Høyesterett i forbindelse med en avskjedssak ta stilling til lovligheten av en arbeidsgivers innsyn i en arbeidstakers brukerområde i datasystemet, foretatt to år etter at informasjon var gitt. Høyesterett fastslo at kontrolltiltaket var rettmessig, men ved vurderingen av rettmessigheten av avskjeden la Høyesterett vekt på at arbeidsgiveren over lengre tid ikke hadde fulgt opp det interne regelverket. Reaksjonen mot arbeidstakeren bar derfor noe preg av vilkårlighet, og avskjeden ble ikke ansett rettmessig. Dette kan tale for at i tilfeller der det er gått lang tid fra informasjon er gitt til tiltaket

[61] Se punkt 1.2.
[62] Arbeidsmiljøloven §§ 4-1 og 4-3.
[63] Ot.prp. nr. 49 (2004-2005) side 314.

iverksettes, vil resultatet av kontrolltiltaket ha begrenset vekt i en etterfølgende oppsigelses- eller avskjedssak. At selve tiltaket er lovlig synes likevel klart.

Bestemmelsen i § 9-2 er kun en ordensregel. Dersom en arbeidsgiver ikke overholder drøftelses- eller informasjonsplikten, blir ikke kontrolltiltaket automatisk ulovlig. Manglende informasjon eller drøfting vil imidlertid i henhold til forarbeidene være et moment i den alminnelige saklighets- og forholdsmessighetsvurderingen,[64] og kan etter omstendighetene medføre at tiltaket anses ulovlig.[65]

3.3.2 Informasjonsplikten i personopplysningsloven

For de kontrolltiltakene som faller innenfor personopplysningslovens virkeområde, suppleres regelen i arbeidsmiljøloven § 9-2 av personopplysningsloven §§ 19 og 20. I henhold til § 19 skal det gis informasjon før det samles inn personopplysninger fra arbeidstakeren selv. Dersom informasjon om en arbeidstaker innhentes fra andre, for eksempel fra kolleger, kan arbeidsgiveren etter § 20 vente med å informere den registrerte til etter at opplysningene er innhentet. I henhold til personopplysningsloven § 18 annet ledd bokstav a kan den det er samlet inn personopplysninger om, i ettertid kreve nøyaktig informasjon om hvilke opplysninger som er samlet inn. Denne rettigheten skal det informeres om i forbindelse med at opplysningene samles inn, jf. §§ 19 og 20.

Som nevnt er informasjonsplikten etter arbeidsmiljøloven § 9-2 bare en ordensregel. Det kan spørres om det samme gjelder reglene i personopplysningsloven §§ 19 og 20. Bestemmelsene i §§ 19 og 20 er en implementering av EUs personverndirektiv art. 10 og art. 11.[66] I henhold til direktivbestemmelsene plikter Norge å fastsette bestemmelser om at den behandlingsansvarlige eller dennes representant *skal* gi informasjon til personer som det innsamles opplysninger fra. Videre følger det av personopplysningsloven § 48 første ledd bokstav f at det å utelate informasjon vil kunne medføre straff for

[64] Se punkt 3.2.1.
[65] Ot.prp. nr. 49 (2004-2005) side 314.
[66] Ot.prp. nr. 92 (1998-1999) side 119.

arbeidsgiveren. Det er altså klart at §§ 19 og 20 statuerer en reell informasjonsplikt. Dermed er det av stor betydning hvorvidt et kontrolltiltak faller innenfor virkeområdet til personopplysningsloven. I så fall vil kontrolltiltaket være i direkte strid med en lovregel hvis ikke arbeidsgiveren gir den nødvendige informasjonen, og tiltaket ikke rammes av noen av unntakene i §§ 19, 20 eller 23.

I tillegg til at arbeidsgiveren risikerer straff, vil lovbruddet ha betydning ved spørsmålet om arbeidsgiveren kan føre resultatene fra kontrolltiltaket som bevis i en senere rettssak. Innen både sivil- og straffeprosessen gjelder den begrensning i prinsippet om fri bevisførsel at utilbørlig ervervet bevis kan nektes ført.[67] Ved utilbørlighetsvurderingen er det av stor betydning om innhentingen av beviset innebar et lovbrudd.

I henhold til § 19 skal arbeidsgivere ved innsamlingen av personopplysninger *"først"* informere den registrerte. Her kan spørsmålet stilles om det kreves informasjon før hvert enkelt tilfelle av innsamling, eller om bestemmelsen skal forstås på samme måte som arbeidsmiljøloven § 9-2. I medhold av § 9-2 holder det som nevnt at informasjon om kontrolltiltak for eksempel gis ved inngåelse av arbeidsavtalen. Ordlyden i § 19 gir ikke inntrykk av at det kreves at informasjon gis før hvert tilfelle av innsamling. I forarbeidene er det tvert imot uttalt at man ved første gangs kontakt med den registrerte kan varsle også om mulighetene for senere innhenting av informasjon, og på den måten gjøre det unødvendig å varsle når informasjonen senere blir samlet inn.[68] Dette innebærer trolig at informasjonsplikten i § 19 som regel er oppfylt dersom en arbeidsgiver ved inngåelsen av et arbeidsforhold gir den nyansatte informasjon i samsvar med § 19 første ledd bokstav a-e, om at personopplysninger fra tid til annen vil bli innhentet på bestemt angitte måter.

[67] Tvisteloven § 22-7 og for eksempel Rt. 1991 side 616.
[68] Ot.prp. nr. 92 (1998-1999) side 43.

4 Kameraovervåking

4.1 Innledning

Et effektivt kontrolltiltak, kanskje særlig for å avsløre og dokumentere mislighold hos en arbeidstaker, kan være å overvåke arbeidsstedet ved hjelp av kameraer koblet til en monitor eller en videoopptaker. Personopplysningsloven kapittel 7 inneholder særlige regler om *"fjernsynsovervåking"*. Disse reglene kan synes å være strengere enn de alminnelige reglene i arbeidsmiljøloven kapittel 9. Blant annet oppstilles det i personopplysningsloven § 38 et vilkår om et *"særskilt behov"* for at fjernsynsovervåking kan godtas. I tillegg følger det av § 40 at det alltid må varsles ved slik overvåking. Av denne grunn er det nødvendig å først fastslå hva som skal til for at kameraovervåking faller inn under kapitlets anvendelsesområde. Dette gjøres i punkt 4.2. Deretter gjøres det rede for i hvilken utstrekning det er adgang til å gjennomføre fjernsynsovervåking av arbeidstakerne i punkt 4.3. I punkt 4.4 vurderes det om det foreligger adgang til skjult kameraovervåking. I dette punktet skilles det mellom tilfellene som faller inn under personopplysningslovens virkeområde og dermed reguleres av varslingsplikten i personopplysningsloven § 40 (punkt 4.4.2), og de som faller utenfor (punkt 4.4.3).

4.2 Personopplysningslovens anvendelsesområde – fjernsynsovervåking

4.2.1 Fjernbetjent eller automatisk virkende kamera

Ikke all overvåking ved bruk av kamera regnes som fjernsynsovervåking i personopplysningslovens forstand. Umiddelbart kan det nevnes at bare overvåking som skjer ved fjernbetjent eller automatisk virkende kamera omfattes av kapitlet, jf. § 36. Det kan dermed ut fra lovens ordlyd fastslås at filming med håndholdt kamera eller stasjonære kameraer som blir manøvrert fra det sted kameraet er plassert, faller utenfor personopplysningslovens virkeområde.

4.2.2 Begrepet personovervåking

For at filming av de ansatte skal regnes som fjernsynsovervåking og dermed rammes av personopplysningslovens regler må det være tale om *"personovervåking"*, jf. § 36. I forarbeidene til den tidligere bestemmelsen om fjernsynsovervåking i straffeloven § 390b er det uttalt at fotografering og filming av bestemte *begivenheter*, selv om dette skulle strekke seg over noe tid, ikke vil ha karakter av overvåking, og følgelig faller utenfor lovreguleringen.[69] Begrepet fjernsynsovervåking i personopplysningsloven samsvarer etter lovens forarbeider med betydningen av samme uttrykk brukt i § 390b.[70] Det kan argumenteres for at filming av en ansatt i forbindelse med en konkret mistanke om mislighold gjelder en bestemt begivenhet, og dermed ikke skal regnes som overvåking. I en kjennelse inntatt i Rt. 2002 side 1572 anførte arbeidsgiveren nettopp dette, at overvåking er noe som går ut over en undersøkelse i en konkret sak. Saken gjaldt straffansvar for en arbeidsgiver på grunn av hemmelig kameraovervåking av en arbeidstaker mistenkt for underslag, og spørsmålet var om overvåkingen var å regne som fjernsynsovervåking etter dagjeldende § 390b i straffeloven. Ettersom begrepet er sammenfallende med samme uttrykk brukt i personopplysningsloven, er kjennelsen relevant ved kartleggingen av hva som regnes som fjernsynsovervåking i personopplysningslovens forstand.

I kjennelsen drøftet Høyesteretts kjæremålsutvalg hvorvidt filming av en arbeidstaker grunnet i en konkret mistanke om straffbare handlinger skulle regnes som *"personovervåking"*. Kjæremålsutvalget viste til bestemmelsens forarbeider, hvor det er klart forutsatt at det kan dreie seg om fjernsynsovervåking også i tilfeller der formålet er å forebygge eller etterforske straffbare handlinger.[71] Kjæremålsutvalget viste også til de strenge reglene som gjelder når politiet benytter skjult kameraovervåking, som argument for at en arbeidsgivers overvåking i etterforskningsøyemed bør regnes som fjernsynsovervåking, med de rettsfølger det innebærer. Det er etter dette klart at skjult

[69] Ot.prp. nr. 56 (1989-90) side 58.
[70] Ot.prp. nr. 92 (1998-99) side 130, jf. Ot.prp. nr. 56 (1992-93) side 29.
[71] Ot.prp. nr. 56 (1992-93) side 10.

kameraovervåking av ansatte, i forbindelse med privat etterforskning, regnes som personovervåking.

4.2.3 Overvåkingen må være vedvarende eller regelmessig gjentatt

Det er bare *"vedvarende eller regelmessig gjentatt"* personovervåking som regnes som fjernsynsovervåking, jf. § 36. Dersom en bestemt arbeidstaker gjentatte ganger filmes når vedkommende er på jobb, vil dette regnes som regelmessig gjentatt personovervåking.

Vanskeligere kan det være å fastslå hva som menes med *"vedvarende"* personovervåking. Selve ordet *"vedvarende"* kan i seg selv signalisere at overvåkingen må foregå over en viss tid. En typisk fremgangsmåte ved konkret mistanke om mislighold vil være korte, målrettede tilfeller av overvåking av enkeltpersoner. Ordlyden i § 36 kan isolert sett tale for at slike tiltak faller utenfor virkeområdet til personopplysningsloven kapittel 7.

Høyesteretts kjæremålsutvalg har tangert spørsmålet i en kjennelse inntatt i Rt. 2004 side 878. På bakgrunn av mistanke om underslag, var en arbeidstaker blitt overvåket med skjult kamera i syv og en halv time én ettermiddag. Spørsmålet i saken var om arbeidsgiveren kunne føre opptakene som bevis i en etterfølgende avskjedssak. Kjæremålsutvalget måtte ta stilling til om bevismidlene var skaffet til veie på ulovlig måte.[72] Ved denne vurderingen var det avgjørende hvorvidt personopplysningslovens regler om fjernsynsovervåking i kapittel 7 kom til anvendelse. Kjæremålsutvalget uttalte at den skjulte overvåkingen i syv og en halv time var *"vedvarende"*. Overvåkingen falt dermed inn under virkeområdet til kapittel 7.

I kjennelsen besvares ikke spørsmålet om hvor kortvarig en overvåkingsseanse må være for ikke å regnes som vedvarende. I forarbeidene til den tidligere bestemmelsen i straffeloven § 390b sies det at overvåking som foretas over kortere tid i forbindelse med etterforskingen

[72] Se punkt 3.3.2 tredje avsnitt.

av en bestemt sak normalt ikke vil regnes som fjernsynsovervåking.[73] Standpunktet er ikke nærmere begrunnet.

I 1993 ble bestemmelsen i § 390b endret. I denne forbindelse ble det uttalt i forarbeidene, riktignok om overvåking av offentlig sted, at overvåking av enkeltstående begivenheter ikke regnes som fjernsynsovervåking. Begrunnelsen var at en viktig rettsfølge av at noe regnes som fjernsynsovervåking, er plikten til å varsle om overvåkingen.[74] Ved enkeltstående begivenheter vil et varslingskrav ifølge forarbeidene være upraktisk og ofte ikke gjennomførbart.[75] Praktiske hensyn er altså med på å begrunne regelen om at bare *"vedvarende"* personovervåking regnes som fjernsynsovervåking i personopplysningslovens forstand.

Ved kameraovervåking av en bestemt arbeidstaker er det ingen praktiske vanskeligheter med å gi varsel, selv om overvåkingen bare er kortvarig. Dette argumentet fremheves av Høyesterett i Rt. 2002 side 1572 som begrunnelse for at overvåkingen i den saken skulle regnes som fjernsynsovervåking. Kjennelsen kan imidlertid ikke ses som et prejudikat for at kriteriet *"vedvarende"* er uten betydning. Resultatet i saken var at kriteriet ble ansett oppfylt, men her var overvåkingen relativt omfattende: det var gjort opptak ved seks anledninger, hver gang på tre timer.

Rimelighetshensyn og likhetshensyn kan tale mot et krav om langvarig overvåking for at den skal regnes som vedvarende. Dersom en ansatt har rullerende oppgaver og for eksempel står en halv time i kassen for så å gå videre til andre arbeidsposter, vil personovervåkingen typisk være tilsvarende kortvarig. Det er vanskelig å finne argumenter for at denne overvåkingen skal falle utenfor personopplysningslovens regler om fjernsynsovervåking. Denne overvåkingen vil kunne oppfattes like krenkende som for en arbeidstaker med lengre skift på én arbeidspost.

---

[73] Ot.prp. nr. 56 (1989-90) side 36.
[74] Varslingsplikten følger nå av personopplysningsloven § 40.

Praktiske og preventive hensyn kan også anføres mot at vilkåret om *"vedvarende"* overvåking skal tolkes strengt. Dersom kortvarig overvåking faller utenfor virkeområdet til personopplysningsloven kapittel 7, vil dette unntaket enkelt kunne påberopes av arbeidsgivere som ikke har oppfylt vilkårene som er oppstilt i kapitlet. Selv om en arbeidsgiver har utført overvåking over lengre tid, er det typisk bare en kort snutt av opptakene som vil være av interesse. Når arbeidsgiveren så i en senere oppsigelsessak eller liknende påberoper seg denne sekvensen av et opptak, vil han kunne hevde at denne er et resultat av kun kortvarig overvåking. Det vil på denne måten være mulig for illojale arbeidsgivere å omgå reglene i kapittel 7. Reelle hensyn tilsier at begrepet vedvarende ikke tolkes strengt.

Det kan innvendes at det i forarbeidene som nevnt klart uttales at overvåking over kortere tid ved etterforskning av en bestemt sak, normalt ikke regnes som vedvarende. Like viktig er kanskje at kravet om varsling ved kameraovervåking av en arbeidstaker kan følge av reglene i arbeidsmiljøloven kapittel 9, selv om overvåkingen ikke formelt regnes som fjernsynsovervåking etter personopplysningsloven § 36. Som nevnt skal arbeidsgiveren gi informasjon om kontrolltiltak, jf. arbeidsmiljøloven § 9-2, men dette er altså bare en ordensregel. Hemmelig overvåking innebærer imidlertid et betydelig inngrep i arbeidstakernes integritet, og vil i henhold til kravet om forholdsmessighet som den klare hovedregel være urettmessig, jf. arbeidsmiljøloven § 9-1. De reelle hensyn som kunne tale mot å innfortolke et krav om lengre varighet i kriteriet *"vedvarende"*, synes dermed ivaretatt gjennom andre regler.

Slik jeg ser det må personovervåkingen etter dette være av en viss varighet for at den skal regnes som *"vedvarende"*. Dersom en arbeidsgiver mistenker en arbeidstaker for underslag og av denne grunn plasserer et kamera i arbeidslokalet rett før arbeidstakeren foretar sluttoppgjør for dagen, vil overvåkingen neppe omfattes av personopplysningslovens regler dersom kameraet fjernes like etter at oppgjøret er avsluttet. I dette tilfellet vil overvåkingen være av så kort varighet at den antagelig ikke kan regnes som vedvarende. Dermed vil

---

[75] Ot.prp. nr. 56 (1992-93) side 12.

overvåkingen ikke omfattes av reglene i personopplysningsloven kapittel 7. For eksempel vil kapitlets vilkår om særskilt behov (§ 38) og varsling (§ 40) ikke komme til anvendelse. På den annen side vil overvåkingen, i medhold av rettspraksis, antas å være vedvarende hvis den varer en hel dag. Den nærmere grensedragningen er uklar. Som nevnt kan gode grunner tale for at det skal relativt lite til før kriteriet *"vedvarende"* er oppfylt. Et moment i vurderingen vil trolig være om overvåkingen gjelder en *bestemt begivenhet*, for eksempel nettopp et sluttoppgjør, eller om overvåkingen har som formål å følge en *person* for å se om vedkommende på en eller annen måte foretar seg noe irregulært.

4.2.4 Unntak ved konkret mistanke om mislighold?

I Rt. 2004 side 878 hevdet arbeidsgiveren at vedkommende hadde konkret mistanke om underslag og at formålet var å skaffe bevis. Dette måtte være til hinder for at reglene i personopplysningsloven kapittel 7 kom til anvendelse. Det ble anført at dette måtte følge av tungtveiende reelle hensyn. Høyesteretts kjæremålsutvalg var ikke enig i dette. Heller ikke etter ordlyden i personopplysningsloven § 36 synes det naturlig å tolke bestemmelsen innskrenkende til ikke å omfatte overvåking som skjer i den hensikt å skaffe seg bevis.

Det må etter kjennelsen legges til grunn at det at kameraovervåking skjer på bakgrunn av mistanke om mislighold av arbeidsavtalen, ikke er til hinder for at overvåkingen regnes som fjernsynsovervåking i henhold til § 36. Kjennelsen i Rt. 2004 side 878 gjaldt et tilfelle der formålet var å skaffe bevis, men forholdet ville neppe stilt seg annerledes om formålet var å få en eksisterende mistanke bekreftet eller avkreftet. I sistnevnte tilfelle kan det hevdes at den ansatte bør ha krav på minst like sterkt personvern, og således vernes av lovens regler, ettersom mistanken mot ham gjerne vil være svakere begrunnet enn i saker der formålet er å skaffe bevis.

4.3 Adgangen til å gjennomføre fjernsynsovervåking

4.3.1 Generelt

I tilfeller der kameraovervåking ikke regnes som fjernsynsovervåking etter § 36, vil rettmessigheten av overvåkingen måtte vurderes alene på bakgrunn av bestemmelsen i arbeidsmiljøloven § 9-1. Oftest vil det imidlertid være tale om fjernsynsovervåking i personopplysningslovens forstand. I disse tilfellene kommer reglene i personopplysningsloven kapittel 7 til anvendelse. I dette punktet vil det redegjøres for i hvilke tilfeller det i medhold av disse reglene er adgang til å gjennomføre fjernsynsovervåking.

4.3.2 Alminnelig overvåking av næringslokale

Personopplysningsloven § 38 regulerer adgangen til fjernsynsovervåking, men er begrenset til å gjelde overvåking av steder der bare en begrenset krets av personer jevnlig ferdes. Ifølge forarbeidene omfattes ikke steder der enhver har adgang. Som eksempel nevnes den delen av en bensinstasjon der kundene har tilgang.[76] Vurderingen av om slik overvåking kan aksepteres må avgjøres alene på bakgrunn av det alminnelige saklighets- og forholdsmessighetsprinsippet.

I forarbeidene til personregisterloven ble det uttalt at for banker må det anses saklig begrunnet at det gjøres opptak i bankens ekspedisjonslokale for å forhindre eller oppklare ran.[77] Høyesterett uttalte i Rt. 2001 side 668 at det ikke kan rettes innvendinger mot alminnelig butikkovervåking som tydelig er varslet. Til dette må det sies at slik overvåking vanligvis er begrunnet i ønsket om å hindre besøkende fra å stjele. Tiltaket mistenkeliggjør altså ikke de ansatte, men kan tvert imot være et verktøy som forenkler arbeidet deres. Det er altså klart at en arbeidsgiver har adgang til å overvåke et næringslokale for å forhindre utenforstående fra å begå tyveri.

[76] NOU 2004: 5 side 429.

4.3.3 Overvåking av arbeidstakere i sikkerhetsøyemed

Fjernsynsovervåking av steder der bare en begrenset krets av personer jevnlig ferdes reguleres som nevnt av personopplysningsloven § 38. Overvåking av områder der det primært er de ansatte som har tilgang vil dermed omfattes. Som eksempel kan nevnes kontor- og fabrikklokaler, personalrom og områder bak kassen på utsalgssteder.

Etter bestemmelsen er slik overvåking bare tillatt dersom det ut fra virksomheten foreligger et *"særskilt behov"*. Som nevnt er det i tillegg et alminnelig vilkår for alle kontrolltiltak at de er saklige og forholdsmessige, jf. arbeidsmiljøloven § 9-1 første ledd. Ved vurderingen av om videoovervåking i en konkret sak er lovlig må man altså se bestemmelsene i personopplysningsloven § 38 og arbeidsmiljøloven § 9-1 i sammenheng. Vilkåret om særskilt behov innebærer at det kreves mer enn hva som følger av det alminnelige saklighetskravet i arbeidsmiljøloven. Dette kan utledes av ordlyden, og følger uttrykkelig av forarbeidene til personregisterloven.[78] Begrepet er ment å ha samme innhold etter personopplysningsloven.[79]

I forarbeidene uttales det at hva som nærmere ligger i begrepet *"særskilt behov"*, må vurderes konkret i relasjon til virksomheten som ønsker å foreta overvåkingen. Det uttales at kravet må anses oppfylt der en bedrift ønsker å foreta overvåking som ledd i arbeidet med å forebygge at farlige situasjoner oppstår, eller av hensynet til ansattes eller andres sikkerhet.[80] Det må til dette presiseres at arbeidsgiveren rent faktisk må ha et særskilt behov for slik overvåking i sikkerhetsøyemed. Det må altså dreie seg om en virksomhet der det er en reell mulighet for at farlige situasjoner vil oppstå. En butikkeier kan dermed ikke overvåke butikkmedarbeiderne under påskudd av at dette gjøres for å ivareta de ansattes sikkerhet. Derimot vil det ved en industribedrift ofte kunne foreligge et behov for å overvåke enkelte områder for å avdekke eller avverge farlige situasjoner.

---

[77] Ot prp. nr. 56 (1992-1993) side 18
[78] Ot prp. nr. 56 (1992-1993) side 18.
[79] Ot.prp. nr. 92 (1998-1999) side 130-131.
[80] Ot prp. nr. 56 (1992-1993) side 18.

4.3.4 Overvåking ved konkret mistanke om mislighold

Et sentralt spørsmål er om en arbeidsgivers konkrete mistanke om mislighold blant de ansatte kan regnes som et særskilt behov for fjernsynsovervåking etter personopplysningsloven § 38. Dernest er spørsmålet om dette behovet veier så tungt at hensynet til de ansattes personvern må vike i vurderingen etter arbeidsmiljøloven § 9-1.

Som nevnt følger det av forarbeidene til arbeidsmiljøloven at det gjelder en vid adgang til å iverksette kontrolltiltak ved konkret mistanke om mislighold.[81] Dette taler for at kameraovervåking i slike tilfeller må aksepteres. Datatilsynet har utarbeidet en veileder om bruk av fjernsynsovervåking. I veilederen heter det at overvåking vil kunne tillates dersom formålet er å motvirke straffbare handlinger fra de ansatte selv, for eksempel underslag eller svinn. Det stilles imidlertid krav til at virksomheten har påvist at slik aktivitet foregår, og til at underslaget eller svinnet er av et visst omfang.[82] Synspunktet harmonerer med arbeidsmiljølovens forarbeider.

Det er imidlertid ikke slik at bare det foreligger en konkret mistanke, er kameraovervåking tillatt. Som nevnt innebærer saklighetsprinsippet i arbeidsmiljøloven § 9-1 et vilkår om forholdsmessighet mellom formålet med kontrolltiltaket og de belastninger dette medfører for arbeidstakerne. Dersom misligholdet det er tale om er marginalt, de ansatte glemmer for eksempel til stadighet å slukke lyset før de går hjem, vil kameraovervåking ikke kunne iverksettes. Underslag, tyveri eller hærverk og andre grove pliktbrudd vil derimot måtte kunne begrunne kameraovervåking.

Videre følger det av saklighetsprinsippet at der et formål kan nås ved forskjellige tiltak, må det minst inngripende tiltaket velges. I forbindelse med underslag kan det tenkes andre hensiktsmessige, mindre inngripende tiltak. Disse vil måtte forsøkes før fjernsynsovervåking kan iverksettes. I tilfeller der det ikke finnes alternative tiltak, er det

[81] Ot.prp. nr. 49 (2004-2005) side 145.
[82] Datatilsynet *"Når har du lov til å overvåke med kamera?"* side 7.

likevel klart at fjernsynsovervåking ved konkret mistanke om mislighold kan aksepteres i medhold av bestemmelsene i personopplysningsloven § 38 og arbeidsmiljøloven § 9-1.

4.4 Særlig om hemmelig kameraovervåking

4.4.1 Innledning

Foreligger konkret mistanke om mislighold, har altså arbeidsgiveren i visse tilfeller adgang til å iverksette kameraovervåking. Et nærliggende spørsmål er om overvåkingen kan skje i det skjulte, eller om de ansatte har krav på varsel i forkant. Kameraovervåking i etterforskingsøyemed vil ofte miste effekten dersom den må varsles på forhånd. Der en arbeidsgiver mistenker en arbeidstaker for regelmessige underslag og ønsker å skaffe bevis for dette, vil overvåking ha liten effekt hvis den mistenkte kjenner til den. På den annen side kan det argumenteres med, slik forarbeidene til arbeidsmiljøloven gjør, at det er politiets oppgave å drive etterforskning,[83] og at dersom overvåkingen bare medfører at det ikke lenger begås underslag, får arbeidsgiveren være fornøyd med det.

4.4.2 Varslingsplikten i personopplysningsloven

I personopplysningsloven § 40 oppstilles det som vilkår for å drive fjernsynsovervåking at det tydelig gjøres oppmerksom på at stedet blir overvåket, typisk ved skilting. Regelen er begrenset til å gjelde fjernsynsovervåking på offentlig sted eller *"sted hvor en begrenset krets av personer ferdes jevnlig"*. En arbeidsplass faller som nevnt i forbindelse med § 38, ofte inn under denne betegnelsen.[84]

Bestemmelsen i § 40 kan tenkes å utgjøre en effektiv skranke mot hemmelig overvåking av arbeidstakere. Etter ordlyden gjelder det ingen unntak fra informasjonsplikten, heller ikke ved etterforskning ved konkret mistanke om mislighold. Verken forarbeidene til personopplysningsloven eller arbeidsmiljøloven gir uttrykk for at regelen kan fravikes ved

[83] NOU 2004: 5 side 430.
[84] Se punkt 4.3.3 første avsnitt.

slik konkret mistanke, men spørsmålet tas heller ikke opp. I kjennelsen i Rt. 2004 side 878 synes Høyesteretts kjæremålsutvalg å legge til grunn at varslingsregelen i § 40 er absolutt. Her måtte kjæremålsutvalget som nevnt vurdere om kameraovervåking i syv og en halv time, på bakgrunn av konkret mistanke om underslag, var å regne som fjernsynsovervåking i personopplysningslovens forstand. Når retten fant at dette var tilfelle, var det samtidig klart at overvåkingen var ulovlig ettersom den ikke var varslet.

Avgjørelsen harmonerer med den nevnte kjennelsen i Rt. 2002 side 1572. Saken gjaldt straffansvar etter den nå opphevede straffeloven § 390b for en arbeidsgiver som hadde bedrevet skjult fjernsynsovervåking av en arbeidstaker, mistenkt for underslag. Etter straffeloven § 390b var det straffbart å foreta fjernsynsovervåking av arbeidssted uten at det var gjort tydelig oppmerksom på at stedet ble overvåket. Personopplysningslovens regler om fjernsynsovervåking bygger som nevnt på den tidligere regelen i straffeloven § 390b.

Høyesteretts kjæremålsutvalg slo først fast at det ikke var gitt varsel før filmingen. Videre ble det vurdert om tiltaket måtte regnes som fjernsynsovervåking. Når kjæremålsutvalget fant at dette var tilfelle, var det klart at varsel skulle blitt gitt. Kjæremålsutvalget åpnet ikke for unntak fra varslingsplikten i tilfeller av konkret mistanke, noe som var påberopt av tiltalte. Det ble tvert imot slått fast at lovgiveren hadde gjort en avveining av de motstridende interessene, og funnet at personvernhensyn måtte veie tyngre enn en arbeidsgivers behov for å drive etterforskning. Etter dette kan det konkluderes med at fjernsynsovervåking i personopplysningslovens forstand må varsles før den iverksettes.

4.4.3 Skjult overvåking når personopplysningsloven ikke kommer til anvendelse

Som nevnt er det ikke alle tilfeller av kameraovervåking som regnes som fjernsynsovervåking i henhold til personopplysningsloven § 36. Det gjelder blant annet der overvåkingen ikke er vedvarende. I disse tilfellene må vurderingen av om overvåkingen kan gjennomføres uten varsel, skje på bakgrunn av reglene i arbeidsmiljøloven. Som nevnt er arbeidsmiljøloven § 9-2 bare en ordensregel. Vurderingen av overvåkingens rettmessighet må derfor foretas på bakgrunn av regelen i § 9-1. Saklighets- og

forholdsmessighetsvilkåret i § 9-1 en kodifisering av etablerte arbeidsrettslige prinsipper. Rettspraksis fra før arbeidsmiljøloven er dermed relevant.

I Rt. 1991 side 616 ble spørsmålet om lovligheten av et opptak gjort ved videoovervåking av en arbeidstaker behandlet. Her var kameraet montert i forståelse med de ansatte, for at de kunne se hva som foregikk i forretningslokalet mens de befant seg på bakrommet. På bakgrunn av iakttakelser arbeidsgiveren gjorde på monitoren på bakrommet, fattet vedkommende mistanke om at en av de ansatte bedrev underslag. Av denne grunn ble kameraet koblet til en opptaker. Spørsmålet i saken var om påtalemyndigheten kunne føre opptakene som bevis. Høyesteretts kjæremålsutvalg måtte følgelig ta stilling til om bevismidlene var skaffet til veie på ulovlig måte.[85]

Ved vurderingen av lovligheten la kjæremålsutvalget vekt på at bruken av kameraet til overvåking av de ansatte måtte anses klart i strid med forutsetningene for ordningen. Videre ble det uttalt ganske generelt at hemmelige videoopptak på arbeidsplassen medfører et slikt inngrep i den personlige integritet at fremgangsmåten ut fra alminnelige personvernhensyn i utgangspunktet bør ansees uakseptabel. Selv om kontrolltiltaket altså var iverksatt på bakgrunn av mistanke om en straffbar handling, ble det ansett ulovlig. Kjennelsen gir klare signaler om at adgangen til hemmelig videoovervåking er svært begrenset.

Denne restriktive holdningen er opprettholdt i flere avgjørelser. Konkret mistanke om ulovlige handlinger er altså ikke nok til at en virksomhet kan drive skjult kameraovervåking, uavhengig av personopplysningslovens regler. Det er uten betydning om bevisene som eventuelt fremkommer skal brukes i en senere sivil- eller straffesak, jf. Rt. 2001 side 668 som gjaldt en avskjedssak.

For at skjult kameraovervåking av arbeidsplassen skal være tillatt, trengs det altså noe mer enn bare en konkret mistanke om for eksempel underslag. Kjennelsen i RG 2002 side 162

er et eksempel på at skjult fjernsynsovervåking ble godtatt og er i flere saker blitt påberopt til inntekt for at inngripende kontrolltiltak må aksepteres. Saken gjaldt hvorvidt to opptak gjort ved skjult fjernsynsovervåking kunne føres i en arbeidsrettssak. Arbeidsgiveren mistenkte at en arbeidstaker slo av den permanente kameraovervåkingen av lokalet for så å ta penger fra kassen. Den permanente overvåkingen gjaldt hele lokalet og falt således ikke inn under personopplysningsloven § 38. Denne overvåkingen var varslet med skilt. For å finne ut hva som foregikk i lokalet, monterte arbeidsgiveren, i tillegg til det permanente anlegget, to skjulte kameraer. Det ene skulle overvåke det samme området som til vanlig var permanent overvåket. Det andre ble montert i skjul i et tilstøtende lokale der det ikke var varslet om overvåking.

Lagmannsretten aksepterte begge opptakene. At det skjulte opptaket fra det til vanlig permanent overvåkede lokalet ble godtatt, er kanskje ikke så overraskende. Opptaket var et resultat av overvåking med skjult kamera i et område som de ansatte visste ble overvåket. Hensikten var å finne ut om det faste kameraanlegget ble satt ut av drift av en arbeidstaker, og om det i denne forbindelse ble begått underslag. Lagmannsretten pekte på at ettersom det var kjent og akseptert av de ansatte at området ble overvåket, utgjorde det supplerende hemmelige opptaket et mindre alvorlig inngrep i personvernet enn det ellers ville gjort. Lagmannsretten uttalte videre at mistanken om manipulasjon av det faste anlegget gjaldt en særlig utspekulert og illojal handlemåte fra en arbeidstaker. Det kan hevdes at dette var momenter som skilte saken i RG 2002 side 162 fra Rt. 1991 side 616.

Det ble imidlertid ikke lagt avgjørende vekt på de ovennevnte momentene. Lagmannsretten fremhevet derimot at formålet med videoopptakene i saken var å avdekke straffbare forhold, og at videoovervåkingen var målrettet og avgrenset i tid og rom. Av disse grunner ble *begge* opptakene godtatt.

Lagmannsretten uttalte at dess sterkere og mer alvorlig en mistanke er, og jo vanskeligere det er å sikre bevis på annen måte, jo lettere er det å akseptere et inngrep i personvernet.

---

[85] Se punkt 3.3.2 tredje avsnitt.

Når det gjelder det andre opptaket, er imidlertid saksforholdet så likt det i Rt. 1991 side 616 at lagmannsrettens vurdering og resultat er lite overbevisende. I Høyesteretts avgjørelser synes det å bli lagt avgjørende vekt på det prinsipielt problematiske i å tillate skjult overvåking. Det er nærliggende å tolke avgjørelsene slik at Høyesterett viker tilbake for å åpne for overvåking i enkelttilfeller, av frykt for den effekten dette kan ha på arbeidslivet generelt. Dersom skjult overvåking godtas bare det hevdes å ha foreligget en konkret mistanke, risikerer man at adgangen vil kunne utnyttes og misbrukes av mange arbeidsgivere.

Det kan med godt belegg hevdes at hovedregelen om at skjult overvåking er ulovlig, skulle kommet til anvendelse på det siste opptaket i saken i RG 2002 side 162. De konkrete omstendighetene rundt det første opptaket, mistanken om det særlig illojale misligholdet samt at de ansatte visste at lokalet normalt ble overvåket, kan derimot hevdes å medføre at dette opptaket måtte anses lovlig, som et unntak fra hovedregelen.

Adgangen til hemmelig kameraovervåking er altså meget snever, også i de tilfellene som ikke rammes av personopplysningslovens kapittel 7. Det kan innvendes at den nevnte praksis fra før personopplysningsloven gjaldt tilfeller av overvåking som i henhold til personopplysningsloven § 36 i dag vil måtte regnes som vedvarende. I Rt. 1991 side 616 var det for eksempel tale om overvåking i 14 timer. Det kan altså hevdes at denne rettspraksisen ikke er relevant ved rettmessighetsvurderingen av kameraovervåking som ikke er regelmessig eller vedvarende. Et motargument er at det i de nevnte avgjørelsene ble lagt liten vekt på varigheten av overvåkingen. I Rt. 1991 side 616 uttalte Høyesterett generelt at hemmelige videoopptak på arbeidsplassen medfører et slikt inngrep i den personlige integritet at fremgangsmåten i utgangspunktet bør ansees uakseptabel. Argumentasjonen og resultatet må dermed sies å ha overføringsverdi til tilfeller av kameraovervåking som faller utenfor personopplysningslovens virkeområde.

5 Innsyn i arbeidstakers e-post og brukerområde i datasystem

5.1 Innledning

I mange arbeidsforhold består en stor del av de ansattes oppgaver i arbeid med datamaskin. Overvåking av de ansattes bruk av maskinene kan dermed være attraktivt sett fra en arbeidsgivers ståsted. I likhet med videoovervåking vil overvåking av datamaskinene være et svært effektivt kontrolltiltak. Det vil kunne gi arbeidsgiveren omfattende informasjon og samtidig være relativt lite ressurskrevende. Arbeidsgiveren kan dessuten fremholde at det er han som eier datautstyret, og at utstyret bare er ment til lojal bruk i jobbsammenheng. Dette kan begrunne en vid adgang til slik kontroll.

På den annen side gjør arbeidstakernes personvernhensyn seg sterkt gjeldende også her. Ved overvåking av e-post eller brukerområde vil ikke arbeidsgiveren se hva den ansatte rent fysisk foretar seg, men derimot hva vedkommende har skrevet og for øvrig benyttet datamaskinen til. Arbeidsgiveren vil blant annet kunne komme over personlige betroelser. I mange tilfeller vil slik overvåking kunne oppfattes som vel så integritetskrenkende som det å bli kameraovervåket.

Det har lenge vært uklart hvilken rettslig adgang en arbeidsgiver har til å overvåke de ansattes bruk av PC. De siste årene er det imidlertid avsagt flere avgjørelser som klargjør rettstilstanden. I tillegg trådte det i kraft 1. mars 2009 et nytt kapittel 9 i personopplysningsforskriften, om innsyn i e-post, personlig brukerområde i datanettverk og annet elektronisk utstyr. Reglene i forskriften er til dels basert på den nevnte rettspraksisen, og kan ses på som en presisering av personopplysningslovens generelt utformede regler, anvendt på innsyn i e-post og liknende.

I dette kapitlet gjøres det i punkt 5.2 rede for anvendelsesområdet til de nye forskriftsbestemmelsene. Deretter gis det i punkt 5.3 en oversikt over tilfeller der innsyn er rettmessig. I punkt 5.4 redegjøres det for reglene om selve gjennomføringen av innsynet,

før det i punkt 5.5 vurderes i hvilken grad arbeidsgiveren må varsle den aktuelle arbeidstakeren i forbindelse med innsyn.

5.2 Anvendelsesområdet til personopplysningsforskriften kapittel 9

En forutsetning for at forskriften kommer til anvendelse, er at innsynet i e-post eller brukerområde i den konkrete saken regnes som behandling av personopplysninger, jf. personopplysningsloven § 3 fjerde ledd første punktum.

Med personopplysninger menes *"opplysninger og vurderinger som kan knyttes til en enkeltperson"*, jf. personopplysningsloven § 2 nr. 1. Formålet med overvåking av ansattes e-post og brukerområde vil nettopp kunne være å finne opplysninger som kan knyttes til enkeltpersoner. I forarbeidene presiseres det at også opplysninger som bare *indirekte* kan identifisere en enkeltperson, regnes som personopplysninger.[86] Dette innebærer at all tekst en arbeidstaker har skrevet, regnes som personopplysninger, forutsatt at leseren på bakgrunn av tekstens innhold forstår hvem forfatteren er.

Det er et spørsmål om ansattes e-postmeldinger alltid regnes som personopplysninger. E-postmeldinger inneholder normalt en identifiserbar adressat og avsender og kan således knyttes til en enkeltperson. Av denne grunn må e-post regnes som personopplysninger. I en kjennelse i Rt. 2002 side 1500 ble det for øvrig lagt til grunn at e-post regnes som personopplysninger, uavhengig av det konkrete innholdet i e-postmeldingene.

Dersom en arbeidsgiver bruker personopplysninger, for eksempel ved å samle inn, registrere eller lagre dem, er det tale om *"behandling"* av personopplysninger, jf. personopplysningsloven § 2 nr. 2. Dette innebærer at der en arbeidsgiver søker opp og samler informasjon produsert av eller om en arbeidstaker, er dette behandling av personopplysninger.

---

[86] Ot.prp. nr. 92 (1998-1999) side 101.

Det kan reises spørsmål om hvor den nedre grensen går for hva som regnes som *behandling* av personopplysninger. Ut fra ordlyden i § 2 nr. 2 kan det for eksempel argumenteres med at selve det å *lese* hva den ansatte har skrevet faller utenfor behandlingsbegrepet. Det kan hevdes at dersom en ansatt går fra datamaskinen sin og arbeidsgiveren ser sitt snitt til å lese hva som står på skjermen, er dette ikke *behandling* av opplysninger. Et motargument er at listen i § 2 nr. 2 over typer av behandling ikke er uttømmende. Det følger allerede av ordlyden at det bare er tale om eksempler. At lesing ikke eksplisitt nevnes i bestemmelsen, er dermed ikke til hinder for at det å lese på den ansattes skjerm skal regnes som *"behandling"*.

Ifølge forarbeidene er begrepet behandling ment å ha et svært vidtrekkende innhold. Det uttales at uttrykket omfatter enhver form for formålsrettet håndtering av personopplysninger.[87] Der en arbeidsgiver snikleser på en arbeidstakers PC-skjerm vil dette som regel skje i den hensikt å tilegne seg personopplysninger. Lesingen utgjør således en formålsrettet håndtering av opplysningene. Uttalelsene i forarbeidene taler altså for at det å lese en ansatts e-post er behandling av personopplysninger i lovens forstand.

I personopplysningsforskriften legges det til grunn at det å *lese* e-post reguleres av forskriften, jf. § 9-2 første ledd. Ettersom forskriften bare gjelder behandling av personopplysninger, jf. personopplysningsloven § 3 fjerde ledd første punktum, synes det som at Fornyings- og administrasjonsdepartementet (FAD)[88] har ansett selve det å *lese* e-post som behandling av personopplysninger. Det å tilegne seg personopplysninger ved lesing, må etter dette regnes som behandling av personopplysninger.

Kontrolltiltak som innebærer behandling av personopplysninger, er det gitt hjemmel til å regulere i forskrift, jf. personopplysingsloven § 3 fjerde ledd første punktum. I personopplysningsforskriften kapittel 9 finnes regler om arbeidsgiveres innsynsrett i

[87] Ot.prp. nr. 92 (1998-1999) side 102.

arbeidstakernes e-post, personlige område i datanettverk og øvrig elektronisk utstyr de ansatte benytter i jobbsammenheng, jf. forskriften § 9-1.

5.3 Situasjoner der innsyn kan foretas

5.3.1 Betydningen av hvem som eier utstyret

En forutsetning for at reglene i forskriften kapittel 9 skal komme til anvendelse, er at utstyret eller e-postkassen er stilt til rådighet av arbeidsgiveren, jf. forskriften § 9-1. Reglene gir under visse omstendigheter arbeidsgiveren rett til innsyn i slikt utstyr. Et spørsmål er om man ut fra en antitetisk tolkning kan slutte at arbeidsgiveren *aldri* har rett til innsyn i utstyr som *ikke* er stilt til rådighet av arbeidsgiver, men som likevel av og til benyttes i arbeidet. Alternativet er at slikt innsyn bare faller utenfor forskriftens virkeområde og at spørsmålet må løses på annet grunnlag.

For en arbeidstaker vil det nok føles mer inngripende om arbeidsgiveren kontrollerer privat e-post og utstyr, enn der kontrollen gjelder utstyr som tilhører arbeidsgiveren. Dette kan tale for et generelt forbud mot innsyn i privat utstyr, selv om det av og til benyttes til arbeidsrelaterte aktiviteter. På den annen side kan det tenkes situasjoner der arbeidstakeren selv besitter spesialutstyr som han også benytter i jobben. Han kan for eksempel konsekvent bruke sin private e-post eller PC. I slike tilfeller kan det, for eksempel ved mistanke om mislighold, synes unaturlig at det avgjørende for en arbeidsgivers innsynsrett, er om utstyret eies av virksomheten eller den ansatte.

FAD har utarbeidet enkelte merknader til bestemmelsene i personopplysningsforskriften kapittel 9.[89] Til forskriften § 9-1 uttales det at arbeidsgivere ikke har innsynrett i dokumenter som er lagret i arbeidstakernes private utstyr, selv om dette fra tid til annen

[88] FAD er gitt kompetanse til å gi forskriftsregler, jf. delegeringsvedtak 11. april 2008 nr. 345, jf. personopplysningsloven § 3 fjerde ledd første punktum.

benyttes til arbeidsrelaterte aktiviteter. [90] Ut fra sammenhengen er det nærliggende å forstå uttrykket privat *"utstyr"* til også å omfatte privat e-postkasse, for eksempel av typen www.hotmail.com. Departementet mener altså at en arbeidsgiver aldri har innsynsrett i disse tilfellene. Et slikt standpunkt innebærer at en arbeidsgiver aldri vil ha adgang til å kontrollere en arbeidstakers private bærbare PC eller private e-postkasse. Det vil heller ikke kunne avtales en slik kontrolladgang. Reglene i forskriften kapittel 9 kan nemlig ikke fravikes til ugunst for arbeidstakeren, jf. § 9-5.

Dersom spørsmålet om innsyn i privat utstyr skulle blitt besvart kun på bakgrunn av de generelt utformede reglene i personopplysningsloven, er det ikke gitt at resultatet ville sammenfalt med departementets standpunkt i merknadene. Etter personopplysnings-loven § 8 bokstav f skal det ved spørsmål om adgangen til å behandle personopplysninger foretas en konkret interesseavveining. Det kan tenkes tilfeller der denne ville slått ut i arbeidsgiverens favør, også ved spørsmålet om innsyn i en arbeidstakers private utstyr. Dette kan for eksempel gjelde dersom den ansatte benytter sin private e-postkasse til å oversende bedriftshemmeligheter til en konkurrerende virksomhet. Dersom arbeidsgiveren har fått mistanke om forholdet kan det hevdes at han vil ha en berettiget interesse i innsyn, og at hensynet til arbeidstakerens personvern ikke overstiger denne interessen. Her vil et absolutt forbud mot innsyn i arbeidstakerens private utstyr kunne oppleves som urimelig.

På den annen side vil arbeidstakerens private PC og e-postkasse som oftest inneholde opplysninger av så privat karakter at det ville føles som et overgrep om arbeidsgiveren skulle ha adgang til å gjennomsøke materialet på jakt etter jobbrelaterte opplysninger. Dette taler for at det ikke bør være opp til arbeidsgiveren å vurdere om rettslig adgang til innsyn foreligger i den enkelte sak, men at det i stedet bør gjelde et absolutt forbud. Til dette kommer at arbeidsgiveren enkelt kan unngå problemene ved et slikt totalforbud, ved å pålegge de ansatte å utelukkende benytte virksomhetens utstyr og e-postsystem når de

---

[89] Se http://www.regjeringen.no/nb/dep/fad/aktuelt/nyheter/2009/fra-i-dag-gjelder-de-nye-reglene-for-inn.html?id=547499.
[90] FADs merknader side 2.

jobber. Det kan etter dette konkluderes med at arbeidsgivere ikke har adgang til å foreta innsyn i de ansattes private e-postkasse eller elektroniske utstyr.

5.3.2 Overvåking og gjennomsøking – administrasjon av systemet

I de fleste tilfeller der en arbeidsgiver ønsker å føre kontroll med en arbeidstakers elektroniske databehandling, vil det aktuelle være innsyn i e-postkasse som arbeidsgiveren har stilt til arbeidstakerens disposisjon eller personlig brukerområde i virksomhetens datanettverk. Med e-postkasse menes i denne sammenheng personlig e-postadresse til bruk i virksomheten, av typen *line.hansen@politiet.no*, tilknyttet egen inn- og utboks for e-postmeldinger. Ved spørsmålet om arbeidsgivere har adgang til å foreta innsyn må det skilles mellom overvåking på den ene siden og innsyn i enkeltstående tilfeller på den andre.

Kontinuerlig overvåking av arbeidstakernes bruk av datamaskin er bare tillatt dersom formålet er administrasjon eller sikring av EDB-systemene, jf. forskriften § 9-2 annet ledd, jf. § 7-11. Dette innbærer blant annet at loggføring av de ansattes bruk kan benyttes til slike formål. Som overvåking regnes også gjennomsøking av datasystemet, for eksempel for å avdekke eventuelle sikkerhetsbrudd, jf. Rt. 2001 side 1589. Et totalforbud mot overvåking ville gjøre det vanskelig for arbeidsgivere å tette sikkerhetshull, typisk ved å spore hvor virus i datasystemene stammer fra. Overvåking eller gjennomsøking i andre øyemed enn administrasjon og sikring av systemet er imidlertid forbudt.[91]

5.3.3 Innsyn for å ivareta en berettiget interesse

Innsyn i enkelttilfeller er lovlig når det er nødvendig for å ivareta en berettiget interesse ved virksomheten, jf. forskriften § 9-2 første ledd bokstav a. Selv om det ikke følger direkte av ordlyden, er det ifølge departementets merknader lagt opp til en interesseavveining av virksomhetens behov for innsyn mot arbeidstakerens behov for personvern.[92] At en slik

[91] Se for eksempel RG 2004 side 347 der arbeidsgiveren hadde gjennomsøkt datasystemet for å avsløre privat bruk av utstyret.
[92] FADs merknader side 2.

interesseavveining må gjennomføres følger for øvrig direkte av personopplysningsloven § 8 bokstav f. Bestemmelsen i forskriften § 9-2 første ledd bokstav a er bare ment som en konkretisering av lovregelen.[93]

Det kan tenkes mange grunner til at en arbeidsgiver vil ønske å undersøke de ansattes e-post, men interessen må være *"berettiget"*, jf. § 9-2 første ledd bokstav a. Som eksempel nevnes den daglige drift av virksomheten. Øvrige eksempler nevnes ikke, men det uttales i merknadene at *"berettiget interesse"* må regnes som en rettslig standard der målestokken må være hva man i alminnelighet anser som legitime hensyn ved en virksomhet.[94] Det er naturlig å se hen til det alminnelige saklighetsprinsippet innen arbeidsretten.[95] Etter ordlyden i forskriftsbestemmelsen er det ikke nærliggende å forstå vilkåret om en berettiget interesse som strengere enn den alminnelige regelen om at en arbeidsgiver må ha et saklig formål begrunnet i virksomheten for å kunne iverksette kontrolltiltak.

Videre er det et vilkår at det er *"nødvendig"* med innsyn for å ivareta arbeidsgiverens berettigede interesse, jf. § 9-2 første ledd bokstav a. Nødvendighetsvilkåret følger for øvrig også av den alminnelige regelen i arbeidsmiljøloven § 9-1 første ledd. Hvorvidt innsyn er nødvendig, må avgjøres etter en konkret vurdering. I merknadene vises det til tilfeller der en arbeidstaker er fraværende fra arbeidet. Dette vil typisk gjelde ved sykdom. Her kan det være viktig for en arbeidsgiver å sjekke, og eventuelt besvare eller videresende, innkomne e-postmeldinger av hensyn til driften av virksomheten. Innen forvaltningen kan det tenkes tilfeller der utenforstående i medhold av offentlighetsloven krever innsyn i dokumenter som befinner seg i e-postkassen til en sykemeldt eller ferierende tjenestemann. [96] I disse tilfellene vil arbeidsgiveren sannsynligvis bli hørt med at innsyn er nødvendig for å oppfylle en berettiget interesse, nemlig forvaltningsorganets plikter utad.

---

[93] FADs merknader side 2.
[94] FADs merknader side 2-3.
[95] Se punkt 3.2.1.
[96] Nina Melsom i Arbeidsrett 2004 nr. 3 side 181.

Ved nødvendighetsvurderingen vil fraværets varighet være et moment, men ikke alene avgjørende. Også ved helt kort fravær, for eksempel en lunsjpause, kan vilkåret ifølge merknadene tenkes oppfylt. Som eksempel nevnes i merknadene tilfeller der arbeidsgiveren har grunn til å tro at det ligger et tilbud med kort akseptfrist i en arbeidstakers e-postkasse, som krever tiltak før arbeidstakeren er tilbake.[97] Motsatt kan det tenkes tilfeller av langvarig fravær der arbeidsgiveren likevel ikke vil ha innsynsrett. Dette kan gjelde der arbeidstakeren ikke er i en posisjon til å binde eller representere virksomheten utad. Her vil det sjelden være nødvendig for arbeidsgiveren å sjekke e-postmeldingene.

Videre ligger det implisitt i vilkåret om nødvendighet at arbeidsgiverens berettigede interesse ikke kan ivaretas på en mindre inngripende måte. Dette fremheves i merknadene.[98] Ofte vil arbeidsgiveren i samarbeid med arbeidstakeren kunne omdirigere e-post i fraværsperioder, eller i det minste sørge for at det sendes ut automatisk svar om at arbeidstakeren ikke er tilgjengelig på arbeidsplassen. Slike tiltak vil være mindre inngripende enn innsyn i den ansattes e-postkasse, og kan dermed hevdes å måtte forsøkes først.

I merknadene fra departementet uttales det at det vil være et element i nødvendighetsvurderingen om *arbeidstakeren* har sørget for slik videresending eller automatisk svar.[99] Departementet synes altså ikke å ville pålegge *arbeidsgiveren* noen aktivitetsplikt i denne henseende. Gode grunner kan imidlertid tale for at det bør være opp til arbeidsgiveren å sørge for at en slik ordning kommer i stand. Dette vil være enkelt for en arbeidsgiver og samtidig lite inngripende overfor arbeidstakeren. Samtidig vil en slik regel være best i samsvar med prinsippet om at det minst inngripende tiltaket må forsøkes først. Det kan i denne sammenheng nevnes at departementet under arbeidet med forskriften har tatt utgangspunkt i den finske loven om integritetsvern i arbeidslivet.[100] I denne loven

---

[97] FADs merknader side 2.
[98] FADs merknader side 2.
[99] FADs merknader side 2.
[100] Se høringsnotat *"Forslag til regler om arbeidsgivers tilgang til ansattes e-post mv."* side 3-4, vedlegg til Høringsbrev av 17.10.2006 fra Fornyings- og administrasjonsdepartementet, se

oppstilles det et eksplisitt vilkår for innsyn i de ansattes e-post, at arbeidsgiveren har lagt til rette for at arbeidstakeren kan videresende e-post eller iverksette liknende tiltak.[101]

Sett i lys av departementets merknader, synes det ikke naturlig å innfortolke noe absolutt vilkår om at arbeidsgiveren har lagt til rette for omdirigering av e-post eller liknende, i bestemmelsen i forskriften § 9-2 første ledd bokstav a. Hvorvidt arbeidsgiveren har gjort dette, vil derimot måtte være et moment i interesseavveiningen. Dersom arbeidsgiveren har anmodet om og lagt til rette for omdirigering, men arbeidstakeren ikke har overholdt anmodningen, vil dette trolig være et moment som taler for at arbeidsgiveren har rett til innsyn.

5.3.4 Innsyn ved berettiget mistanke om pliktbrudd

5.3.4.1 Innledning

I tilfeller der arbeidsgiveren har en berettiget mistanke om at en arbeidstakers bruk av e-postkassen eller datasystemet medfører et grovt brudd på pliktene som følger av arbeidsforholdet eller kan gi grunnlag for oppsigelse eller avskjed, har arbeidsgiveren alltid rett til å foreta innsyn, jf. forskriften § 9-2 første ledd bokstav b. Regelen samsvarer med uttalelsene i arbeidsmiljølovens forarbeider om at det gjelder en vid adgang til kontrolltiltak ved konkret mistanke om straffbare handlinger eller mislighold av arbeidsavtalen.[102] I merknadene til forskriftsbestemmelsen nevnes noen eksempler på forhold som kan begrunne en innsynsrett. Det presiseres at det ikke gjelder noe vilkår om at arbeidstakeren har gjort seg skyldig i straffbare forhold, men det må gjelde handlinger som åpenbart ikke er i virksomhetens interesse. Nedenfor nevnes enkelte forhold som kan begrunne innsynsrett.

---

http://www.regjeringen.no/nb/dep/fad/dok/Horinger/Horingsdokumenter/2006/forslag-til-regler-om-arbeidsgivers-adga/1.html?id=270943.

[101] Lag om integritetsskydd i arbetslivet 13.8.2004/759 § 18.

[102] Ot.prp. nr. 49 (2004-2005) side 145.

5.3.4.2 Arbeidstakeren misbruker e-postkontoen

I departementets merknader nevnes utsendelse av spam som et forhold som kan begrunne innsyn i arbeidstakerens e-postkasse.[103] Spam er en betegnelse på uønsket reklame og annen masseutsendt informasjon som ikke er godkjent av mottakeren. Distribusjon av slik e-post vil kunne sette virksomheten i et dårlig lys, og kan av denne grunn anses som et grovt brudd på den alminnelige lojalitetsplikten i arbeidsforhold.

Videre nevnes i merknadene tilfeller der arbeidsgiverens utstyr benyttes til trakassering av kolleger.[104] Det må til dette påpekes at arbeidsgivere har en plikt til å sørge for at de ansatte ikke utsettes for trakassering, verken fra arbeidsgiveren selv eller fra kollegene, jf. arbeidsmiljøloven § 4-3 tredje ledd, jf. § 2-1. Dessuten er arbeidsgiveren i medhold av skadeerstatningsloven § 2-1 objektivt ansvarlig for skade som følge av mobbing fra andre arbeidstakere, jf. Rt. 1997 side 786. Der en arbeidstaker trakasserer en kollega, hindrer vedkommende arbeidsgiveren fra å oppfylle sine plikter, og kan samtidig påføre arbeidsgiveren et direkte økonomisk tap. Dette innebærer et klart brudd på lojalitetsplikten og kan dermed begrunne innsyn i e-post eller personlig brukerområde i datasystemet.

5.3.4.3 Nedlasting av pornografisk materiale

Nedlasting av ulovlig materiale eller ulovlig fildeling, nevnes også i merknadene som eksempler på forhold som kan begrunne innsyn. Det er presisert at barnepornografisk materiale omfattes.[105] Selv om nedlasting av barnepornografi er moralsk forkastelig og straffbart, er det ikke innlysende at mistanke om slike forhold gir arbeidsgiveren rett til innsyn i arbeidstakerens e-post eller brukerområde i datasystemet. Spørsmålet er om slik nedlasting kan sies å utgjøre et grovt pliktbrudd overfor arbeidsgiveren, jf. forskriften § 9-2 første ledd bokstav b.

---

[103] FADs merknader side 3.
[104] FADs merknader side 3.
[105] FADs merknader side 3.

Spørsmålet er behandlet i en avgjørelse fra Oslo tingrett.[106] I forbindelse med en avskjedssak måtte retten ta stilling til lovligheten av innsyn i en arbeidstakers private filer lastet ned i arbeidsgiverens datasystem. Arbeidsgiveren hadde under et søk etter noen savnede filer, kommet over enkelte mistenkelige filer i systemet. Arbeidsgiveren åpnet disse, som viste seg å inneholde barnepornografiske bilder. Retten fant på bakgrunn av personopplysningsloven § 8 bokstav f, at arbeidsgiveren hadde lovlig adgang til å åpne filene. I interesseavveiningen la retten vekt på at arbeidstakeren hadde benyttet arbeidsgiverens utstyr til straffbar virksomhet. Det ble også fremhevet at arbeidsgivere har en straffesanksjonert plikt til å forhindre at de ansatte befatter seg med barnepornografi i virksomheten, jf. nå straffeloven § 204a tredje ledd. Videre ble det lagt vekt på at arbeidsgiveren hadde gitt klare instrukser om at slik nedlasting var uakseptabelt, og at man ville prøve å finne frem til den skyldige dersom slikt materiale ble funnet.

I likhet med det som er sagt om betydningen av å legge til rette for omadressering av e-post ved fravær, fant retten altså at det også her har betydning at arbeidsgiveren hadde gitt den ansatte en klar instruks, og at denne var overtrådt. Rettens argumentasjon er overbevisende. Jeg vil derfor anta at dommen gir uttrykk for gjeldende rett. Vurderingen vil for øvrig måtte bli den samme i henhold til personopplysningsforskriften § 9-2 første ledd bokstav b.

I tilfeller der det ikke er gitt noen advarsel om at nedlasting av barneporno er forbudt og vil etterforskes, er det ikke like åpenbart at en arbeidsgiver kan foreta innsyn ved mistanke om slik virksomhet. Det kan hevdes at nedlastingen da ikke vil innebære et grovt pliktbrudd, og at vilkårene for innsyn i henhold til forskriften § 9-2 ikke er oppfylt. Dette synspunktet underbygges av at en arbeidsgiver neppe har noen straffesanksjonert plikt til følge opp avdekking av barnepornografi med en personalsak. Arbeidsgiverens plikter etter straffeloven § 204a vil trolig være oppfylt ved klare instrukser og pålegg om å slette filer man antar kan inneholde ulovlig materiale. [107]

[106] TOSLO-2001-12516.
[107] TOSLO-2001-12516 niende avsnitt av rettens bemerkninger.

På den annen side taler det for en alminnelig regel om innsynsrett ved mistanke om befatning med barnepornografi, at det dreier seg om straffbare handlinger ved bruk av arbeidsgiverens utstyr. Forholdet vil kunne sette arbeidsgiveren i et dårlig lys, og virksomheten risikerer å bli assosiert med saken i lang tid. Dette hensynet kan sies å gjelde særlig sterkt ved nedlasting av barnepornografi. Slikt materiale vekker gjerne sterkere negative reaksjoner i befolkningen enn annen ulovlig nedlasting, for eksempel av musikk. På denne måten medfører nedlastingen en fare for tap av anseelse og økonomiske skadevirkninger for arbeidsgiveren. Dette taler for at slik nedlasting innebærer et grovt brudd på lojalitetsplikten og dermed innsynsrett.

Preventive hensyn kan også fremheves. Dersom arbeidstakeren vet at arbeidsgiveren ved mistanke har adgang til å kontrollere filene hans, vil det kunne gjøre det mindre forlokkende å laste ned barnepornografien. På bakgrunn av disse sterke reelle hensynene må det kunne konkluderes med at en arbeidsgiver har adgang til å foreta innsyn ved mistanke om at en arbeidstaker har lagret barnepornografi i datasystemet.

Også ved mistanke om at arbeidstakeren har lastet ned og lagret "vanlig" pornografi i datasystemet kan rett til innsyn foreligge. I dommen inntatt i Rt. 2005 side 518 var dette et spørsmål. Arbeidsgiveren hadde søkt generelt i datasystemet etter filer med pornografisk innhold, også inne på de enkelte brukernes område. Bakgrunnen ble hevdet å være at slike filer utgjorde en risiko for virusangrep. Høyesterett vurderte spørsmålet i lys av personopplysningsloven § 8 bokstav f og kom til at innsynet var rettmessig. Det ble fremhevet at nedlastingen var i klar strid med bedriftens regler og at arbeidsgiveren hadde hatt en saklig begrunnet oppfatning om at slik aktivitet utgjorde en reell sikkerhetsrisiko. Av Høyesteretts uttalelser er det nærliggende å utlede at det ved mistanke om nedlasting av pornografi er et vilkår for innsyn at det på forhånd er varslet at slik nedlasting er forbudt. Dette kan også sies å følge direkte av vilkåret om *"grovt pliktbrudd"* i forskriften § 9-2 første ledd bokstav b. Nedlasting av vanlig pornografi er ikke ulovlig,[108] og slik

[108] Sml. straffeloven § 204.

virksomhet kan som utgangspunkt neppe begrunne en oppsigelse.[109] I underrettspraksis finnes også eksempler på at innsyn ble funnet urettmessig ettersom det ikke var fastlagt ordensregler for bruken av datautstyret.[110]

Det må videre nevnes at selve gjennomsøkingen av datasystemet i saken i Rt. 2005 side 518 var begrunnet i sikkerhetsmessige hensyn. Dette er i tråd med den nye bestemmelsen i personopplysningsforskriften § 9-2 annet ledd, jf. § 7-11.[111]

5.3.4.4 Ulovlig fildeling

I merknadene nevnes ulovlig fildeling som et forhold som kan begrunne rett til innsyn. Dette vil typisk gjelde nedlasting og deling av filmer og musikk fra internett. Høyesterett måtte i dommen inntatt i Rt. 2001 side 1589 ta stilling til om en arbeidsgiver hadde adgang til å ta utskrift av innholdet i harddisken til PC'en til en arbeidstaker. Arbeidsgiveren mistenkte arbeidstakeren for nedlasting i stort omfang, noe som førte til treghet i systemet. På bakgrunn av mistanken låste arbeidsgiveren seg inn på den ansattes kontor, undersøkte PC'en og tok utskrift. Arbeidsgiverens opptreden var rettmessig. Høyesteretts begrunnelse var imidlertid ganske konkret idet det ble vektlagt at det på det aktuelle arbeidsstedet var vanlig og akseptert at de ansatte gikk inn på hverandres kontorer og til dels brukte hverandres PC'er.

Generelt må det likevel kunne sies å være legitimt for en arbeidsgiver å søke å få best mulig utnyttelse av internettlinjen. Dersom man har holdepunkter for at en arbeidstaker misbruker systemet, kan dette begrunne innsyn. Her vil likevel kravet som følger av arbeidsmiljøloven § 9-1, at mindre inngripende tiltak må benyttes først, spille inn. Ofte vil det være nok å gjøre det klart for de ansatte at det ikke er adgang til for eksempel å laste ned musikk. Dersom forbudet ikke overholdes, vil innsyn kunne være rettmessig.

---

[109] Se for eksempel RG 2004 side 198.
[110] Se for eksempel RG 2004 side 347.
[111] Se punkt 5.3.2.

5.3.4.5 Illojal opptreden

Merknadenes liste over eksempler er etter sin ordlyd ikke ment å være uttømmende. Også forhold som ikke er spesifikt nevnt kan begrunne rett til innsyn såfremt det er tale om et grovt pliktbrudd. Eksempler kan være mistanke om uberettiget fravær eller at en ansatt i skjul sørger for å få betalt for flere timer enn vedkommende faktisk arbeider. Her vil det kunne være rettmessig å foreta innsyn i arbeidstakerens datalogg.[112]

Hvis arbeidsgiveren mistenker en arbeidstaker for å lekke informasjon eller for å illojalt forsøke å føre kunder over til en konkurrerende virksomhet, vil dette kunne begrunne innsyn. Overføring av informasjon og kunder til en konkurrerende virksomhet kan sies å være uttrykk for illojalitet i sin reneste form, og kan utvilsomt begrunne oppsigelse eller avskjed. I en kjennelse inntatt i Rt. 2002 side 1500 fant Høyesteretts kjæremålsutvalg at innsyn i en arbeidstakers e-postkasse tilknyttet virksomheten var rettmessig. Bakgrunnen var mistanke om at arbeidstakeren hadde fått tilbud om ansettelse i et konkurrerende selskap, og at han forsøkte å ta med seg kunder til sin nye arbeidsgiver.

5.3.4.6 Betydningen av at e-post er virksomhetsrelatert

Sett i lys av de nye reglene i forskriften kapittel 9 er det enkelte forhold ved avgjørelsen inntatt i Rt. 2002 side 1500 som må kommenteres. Lagmannsretten hadde ved vurderingen av rettmessigheten av innsynet lagt avgjørende vekt på om e-postmeldingene var virksomhetsrelaterte. Ettersom dette var tilfellet, måtte innsynet godtas. Høyesteretts kjæremålsutvalg presiserte at det rettslige grunnlaget for løsningen av spørsmålet var personopplysningsloven § 8 bokstav f, men at de elementene lagmannsretten hadde lagt vekt på var dekkende også i relasjon til vurderingen etter lovbestemmelsen. Kjæremålsutvalget kom til at e-postene var virksomhetsrelaterte og at lagmannsretten ikke hadde begått feil ved lovanvendelsen.

[112] Se for eksempel LB-2007-121782.

For det første synes resultatet, at innsynet var rettmessig, å kunne forsvares også dersom man tar utgangspunkt i forskriften § 9-2 første ledd bokstav b. Det var tale om mistanke om forhold som utgjorde grove brudd på de plikter som fulgte av arbeidsavtalen. Derimot synes ikke begrunnelsen ved første øyekast å samsvare helt med de vilkår som nå følger av forskriften kapittel 9. I dommen fra lagmannsretten var det blitt lagt avgjørende vekt på om e-posten var virksomhetsrelatert. Høyesteretts kjæremålsutvalg uttalte at dersom det var tale om slik virksomhetsrelatert e-post, ville arbeidsgiveren ha en *"berettiget interesse"* i å foreta innsyn, jf. personopplysningsloven § 8 bokstav f. Kjæremålsutvalget uttalte videre at utvalget ikke kunne prøve lagmannsrettens konkrete vurdering. Med dette siktet kjæremålsutvalget øyensynlig til interesseavveiningen av arbeidsgiverens berettigede interesse satt opp mot den ansattes personvern.

Kjennelsen er i teorien blitt forstått slik at en arbeidsgiver som det klare utgangpunkt har adgang til å kontrollere virksomhetsrelatert e-post.[113] Også arbeidslivslovutvalget uttalte i forbindelse med arbeidet med arbeidsmiljøloven at en arbeidsgiver har en berettiget interesse i å lese virksomhetsrelatert e-post, og at denne interessen overstiger hensynet til arbeidstakerens personvern.[114]

Et slikt standpunktet harmonerer dårlig med den nye regelen i personopplysningsforskriften § 9-2. Her stilles det som vilkår for innsyn at dette må være nødvendig eller at det må foreligge konkret mistanke om mislighold. Også i lys av det alminnelige saklighetsprinsippet synes det tvilsomt at en arbeidsgiver skal ha adgang til å foreta innsyn i de ansattes e-postkasser og lese e-post, bare den er virksomhetsrelatert. For arbeidstakere vil dette kunne oppleves som et integritetskrenkende kontrolltiltak. I tråd med arbeidsmiljøloven § 9-1 kan det hevdes at mindre inngripende tiltak må forsøkes først.

Datatilsynet fremholder på sine hjemmesider om rettstilstanden før ikrafttredelsen av forskriften kapittel 9, at det *"vil finnes situasjoner"* hvor arbeidsgiveren har en saklig

[113] Se Jakhelln (2006) side 404-405.
[114] NOU 2004: 5 side 428.

begrunnelse for å gjennomgå den ansattes e-postkasse på utkikk etter virksomhetsrelatert post.[115] Som eksempel nevner Datatilsynet tilfeller der den ansatte er fraværende over lengre tid. Tilsynet synes altså ikke å mene at en arbeidsgiver som utgangspunkt har anledning til å kontrollere virksomhetsrelatert e-post. I sin praksis har også Datatilsynet lagt til grunn at det ikke er tilstrekkelig for å anse en arbeidsgivers interesse i innsyn som *"berettiget"*,[116] at det dreier seg om virksomhetsrelatert e-post.[117]

Etter ovennevnte drøftelse, er det etter min oppfatning ikke alene avgjørende for spørsmålet om rettmessigheten av innsyn, om en e-post er virksomhetsrelatert eller ikke. En arbeidsgiver må i det konkrete tilfellet i tillegg påvise en saklig grunn for innsynet, enten at det foreligger en mistanke om mislighold eller at innsynet er nødvendig for å ivareta en annen berettiget interesse, jf. forskriften § 9-2 første ledd.

5.3.4.7 Mistanken må være begrunnet

For at en arbeidsgiver skal kunne foreta innsyn i e-postkassen eller datamaskinen til en arbeidstaker som mistenkes for grovt pliktbrudd, må mistanken være *"begrunnet"*, jf. forskriften § 9-2 første ledd bokstav b. Ettersom adgangen til innsyn er større ved konkret mistanke, er det naturlig at det stilles vilkår om at mistanken må være begrunnet. I motsatt fall ville en arbeidsgiver alltid, som et vikarierende motiv, kunne påberope seg en mistanke mot de arbeidstakere han av ulike grunner ønsket å foreta innsyn hos.

I merknadene til bestemmelsen uttales det at arbeidsgiveren må ha mer enn en løselig antakelse. Han må ha konkret informasjon som gir grunn til å tro at e-postkassen eller brukerområdet inneholder opplysninger som kan føre til oppsigelse eller avskjed. Som

[115] Se http://www.datatilsynet.no/templates/article____201.aspx punktet "Klare retningslinjer for bruk av datasystemet".
[116] Jf. personopplysningsloven § 8 bokstav f.
[117] Se for eksempel sak 2005/1193 *Datatilsynet–Bazar forlag* dok. 23 side 7.

eksempler nevnes tips fra kolleger eller informasjon fremkommet gjennom den generelle administrasjonen av virksomhetens IT-systemer, jf. forskriften § 7-11.[118]

Departementet mener altså at opplysninger som er fremkommet gjennom overvåking eller gjennomsøking av datasystemet i den hensikt å administrere det, kan benyttes av arbeidsgiveren som begrunnelse for å foreta innsyn i den enkelte arbeidstakers e-postkasse. Dette kan synes overraskende når det samtidig følger av § 7-11 tredje ledd at personopplysninger som fremkommer ved slik administrativ overvåking ikke senere kan *"behandles for å overvåke eller kontrollere den enkelte"*. Isolert sett tilsier ordlyden at opplysninger fremkommet gjennom administrativ overvåking, ikke kan benyttes til noe annet formål enn nettopp sikkerhet eller administrasjon av EDB-systemet.

Det følger imidlertid av Høyesteretts praksis at bestemmelsen i § 7-11 neppe kan forstås slik. I samtlige av de nevnte avgjørelsene fra Høyesterett om innsyn i e-post eller brukerområde i datasystemet, var mistanken en følge av funn gjort ved administrativ gjennomsøking i tråd med forskriften § 9-2 annet ledd, jf. § 7-11. Høyesterett fant i samtlige avgjørelser at opplysninger fremkommet ved slik legitim gjennomsøking kunne begrunne ytterligere innsyn.

I dommen i Rt. 2005 side 518 godtok Høyesterett at pornografisk materiale fremkommet ved gjennomsøking av datasystemet i sikkerhetsøyemed, ble brukt av arbeidsgiveren i en senere avskjedssak. Høyesterett kunne ikke se at dette var i strid med § 7-11 tredje ledd. Datatilsynet uttalte seg i anledning saken og la vekt på at det aktuelle misligholdet var et så klart brudd på fastsatte retningslinjer at det ville være urimelig om arbeidsgiveren skulle være avskåret fra å aksjonere.[119]

I dommen inntatt i Rt. 2001 side 1589 hadde arbeidsgiveren undersøkt en arbeidstakers PC på grunn av mistanke om omfattende musikknedlasting. Mistanken skyldtes funn gjort ved

[118] FADs merknader side 3.
[119] Rt. 2005 side 518 avsnitt 56.

gjennomsøking av datasystemet begrunnet i et ønske om å finne årsakene til treghet i systemet. Høyesterett uttalte at dagjeldende personregisterforskrift § 2-20 ikke var til hinder for at arbeidsgiveren brukte personopplysninger han fant ved gjennomsøkingen som begrunnelse for å foreta ytterligere innsyn. I følge merknadene til personopplysningsforskriften § 7-11 er denne bestemmelsen en videreføring av innholdet i personregisterforskriften § 2-20.[120] Dette taler for at Høyesteretts bemerkninger har betydning også etter innføringen at § 7-11. At rettstilstanden er videreført er lagt til grunn i underrettspraksis.[121]

Bestemmelsen i personopplysningsforskriften § 7-11 tredje ledd er imidlertid ny sammenlignet med den i personregisterloven § 2-20. I merknadene til § 7-11 uttaler departementet at formålsangivelsen i tredje ledd er tatt med for å klargjøre at loggopplysninger ikke kan brukes til for eksempel administrative tiltak overfor de enkelte ansatte. Denne uttalelsen kan ved første øyekast være noe vanskelig å forene med dommen i Rt. 2005 side 518, der en arbeidstaker ble utsatt for et administrativt tiltak på bakgrunn av funn gjort ved en generell gjennomsøking av lagrede filer. Likevel kan det sies å være en viktig forskjell mellom faktum i dommen og den situasjonen som beskrives i merknadene. Det kan hevdes å være av større betydning for en arbeidsgiver hva de ansatte har lagret av materiale i datasystemet, enn for eksempel hvilke internettsider de har besøkt. Det er jo nettopp slike loggopplysninger departementet uttaler seg om. Dette taler for at det ikke er noe motsetningsforhold mellom Høyesteretts syn i Rt. 2005 side 518 og departementets syn i merknadene til § 7-11.

Slik jeg ser det, kan opplysninger fremkommet ved gjennomsøking av eksisterende *filer i datasystemet*, med et administrativt formål, begrunne videre innsyn for eksempel i den ansattes brukerområde i datasystemet eller e-postkasse. Dersom en arbeidsgiver derimot skulle gjennomsøke de ansattes *internettlogg* og for eksempel komme over hyppige besøk på pornonettsider, er det derimot tvilsomt om dette i seg selv ville kunne begrunne videre

[120] Se merknadene fra Justis- og politidepartementet (JD) til § 7-11.
[121] TOSLO-2001-12516 fjerde til sjette avsnitt av rettens bemerkninger.

innsyn i den ansattes brukerområde eller andre administrative tiltak. Her kan det, sett i lys av merknadene, hevdes at departementet gjennom bestemmelsen i forskriften § 7-11 tredje ledd har latt hensynet til den ansattes personvern veie tyngre enn arbeidsgiverens ønske om å finne ut mer om sin arbeidstaker. [122] En slik regel er også best i samsvar med formålet bak personvernlovgivningen, å sikre den personlige integritet, jf. personopplysningsloven § 1.

5.4 Gjennomføringen av innsynet

Forskriften § 9-3 inneholder enkelte regler om selve gjennomføringen av innsyn. I henhold til § 9-3 fjerde ledd må innsyn gjennomføres på en slik måte at dataene så langt mulig ikke endres. Frembrakte opplysninger må kunne etterprøves. Dette er selvfølgelig viktig av kontradiktoriske hensyn. Regelen kan samtidig sies å presisere formålsbestemmelsen i personopplysningsloven § 1. Her fremheves behovet for tilstrekkelig kvalitet på personopplysningene når de behandles, jf. § 1 annet ledd. Norge plikter for øvrig å ha regler som pålegger den som behandler personopplysninger å sikre kvaliteten på opplysningene, jf. EUs personverndirektiv art. 6.

I underrettspraksis er det blitt uttrykt at en arbeidsgivers behandling av personopplysninger må oppfylle visse kvalitetskrav. I en dom fra Borgarting lagmannsrett ble arbeidsgiverens behandling av logginformasjon fra en arbeidstakers datamaskin ansett å være lovstridig.[123] Bakgrunnen var at innsamlet informasjon ble brukt som grunnlag for å underbygge påstander om uberettiget fravær. Når metoden arbeidsgiveren hadde benyttet led av betydelige svakheter, og det resultatet arbeidsgiveren presenterte dermed ikke var pålitelig, måtte behandlingen av personopplysningene etter en samlet vurdering anses å være i strid med personopplysningsloven § 8. I dag vil resultatet kunne forankres i personopplysningsforskriften § 9-3 fjerde ledd.

---

[122] JDs merknader.
[123] LB-2007-121782.

Dersom arbeidsgiveren har foretatt innsyn i en arbeidstakers e-postkasse, men det viser seg at den ikke inneholder dokumenter arbeidsgiveren har innsynsrett i, skal e-postkassen og øvrige dokumenter straks lukkes. Dette følger naturlig av det alminnelige saklighetsprinsippet og er nå direkte uttrykt i forskriften § 9-3 femte ledd.

5.5 Varslings- og informasjonsplikt

5.5.1 Innledning

Det følger som nevnt av arbeidsmiljøloven § 9-2 at en arbeidsgiver plikter å informere og foreta drøftelser med de ansatte før et kontrolltiltak iverksettes. Dette er imidlertid bare en ordensregel. Brudd på informasjons- og drøftelsesplikten etter denne bestemmelsen medfører ikke automatisk at innsyn i en arbeidstakers e-postkasse er ulovlig.[124] Dessuten innebærer ikke denne bestemmelsen at en arbeidsgiver plikter å informere om hvert enkelt kontrolltiltak.[125] Personopplysningsforskriften inneholder imidlertid særregler om hvilke prosessuelle plikter en arbeidsgiver har i forbindelse med innsyn i e-post, brukerområde i datasystem og annet elektronisk utstyr.

5.5.2 Utgangspunktet – varsel før innsyn foretas

I henhold til forskriften § 9-3 første ledd skal en arbeidstaker varsles før innsyn foretas og gis anledning til å uttale seg. Videre skal vedkommende gis anledning til å være til stede ved gjennomføringen av innsynet sammen med en representant. Varslingsplikten er ikke absolutt, den gjelder bare *"så langt mulig"*. I departementets merknader til bestemmelsen uttales det at varsling for eksempel kan utelates dersom det er nødvendig å foreta innsyn umiddelbart, og arbeidsgiveren ikke har tid til å kontakte arbeidstakeren.[126] Dette vil for eksempel kunne gjelde der arbeidsgiveren har grunn til å tro at det ligger et tilbud med kort

[124] Se punkt 3.3.1.
[125] Se punkt 3.3.1.
[126] FADs merknader side 4.

akseptfrist i arbeidstakerens e-postkasse, og arbeidstakeren er utilgjengelig. Dersom arbeidsgiveren derimot har tid til å kontakte arbeidstakeren, må dette gjøres.[127]

I tilfeller der en arbeidsgiver ønsker å foreta innsyn grunnet i en mistanke om at arbeidstakeren har lagret e-post eller annet materiale som innebærer et grovt pliktbrudd, kan han frykte at arbeidstakeren vil endre eller slette materialet dersom han blir varslet om kontrolltiltaket. Her kan det være fristende å unnlate varsling. I departementets merknader til bestemmelsen pekes det på at arbeidsgiveren i stedet kan foreta en speilkopiering av områdene i det elektroniske nettverket det er rettslig grunnlag for å foreta innsyn i. På denne måten vil arbeidsgiveren ha et riktig øyeblikksbilde av materialet som han kan gå tilbake til ved mistanke om at noe er endret. Etter å ha gjennomført speilkopieringen kan arbeidsgiveren varsle den ansatte om at innsyn vil bli foretatt og at vedkommende kan være tilstede.[128] Dette er i tråd med prinsippet om at der det foreligger alternativer, skal det minst inngripende tiltaket velges.

I den nevnte rettspraksis er imidlertid muligheten til å foreta speilkopiering fremfor direkte innsyn uten forutgående varsel, ikke blitt fremhevet som argument for at innsynet har vært ulovlig. Rettspraksis har altså vært mer liberal overfor arbeidsgiverne enn den regelen som departementet legger opp til med innføringen av nye § 9-3. At speilkopiering er et alternativ, fremkommer heller ikke direkte av ordlyden i § 9-3. Det kan neppe forutsettes at alle arbeidsgivere kjenner til denne muligheten. Dette taler mot at ikkevarslede innsyn alltid skal være ulovlig i tilfeller der speilkopiering rent faktisk kunne vært et alternativ. Gode grunner kan tale for at det må vurderes konkret hvorvidt en arbeidsgiver burde ha foretatt speilkopiering fremfor å gjennomføre innsyn uten varsel.

[127] FADs merknader side 4.
[128] FADs merknader side 4.

5.5.3 Etterfølgende varsel

I tilfellene der innsyn er gjennomført uten at det har vært mulig å varsle, plikter arbeidsgiveren å gi arbeidstakeren skriftlig underretning om innsynet så snart dette er gjennomført. Her skal grunnlaget for innsynet, metoden som er blitt brukt og resultatet av innsynet nevnes. Videre skal det opplyses om hvilke rettigheter arbeidstakeren har i forbindelse med tiltaket, jf. § 9-3 annet ledd. På denne måten vil arbeidstakeren kunne ta stilling til om vedkommende er enig i arbeidsgiverens vurdering av at det forelå rettmessig adgang til innsyn og at varsling i forkant ikke var påkrevd.

5.5.4 Unntak fra varslingsplikten

I henhold til forskriften § 9-3 tredje ledd gjelder personopplysningsloven § 23 om unntak fra informasjonsplikten tilsvarende for forutgående og etterfølgende varsling ved innsyn i e-post og elektronisk utstyr. Det følger av § 23 første ledd bokstav b at informasjon kan unnlates dersom det er påkrevd av hensyn til forebygging, etterforskning, avsløring og rettslig forfølgning av straffbare handlinger. Etter ordlyden kunne denne bestemmelsen synes aktuell for arbeidsgivere som for eksempel mistenker en ansatt for å bedrive underslag og ønsker å iverksette privat etterforskning.

I henhold til forarbeidene til § 23 første ledd bokstav b er det imidlertid politiets og enkelte andre kontrolletaters etterforskning det siktes til i bestemmelsen.[129] Likevel vises det til § 23 i forskriften § 9-3. Dette indikerer at også en arbeidsgiver kan påberope seg § 23, ettersom forskriften kapittel 9 bare gjelder *arbeidsgiveres* rett til innsyn i arbeidstakers e-postkasse, jf. forskriften § 9-1 første ledd. I motsatt fall kan det stilles spørsmålstegn ved hvorfor det i det hele tatt vises til personopplysningsloven § 23.

I merknadene til forskriften § 9-3 tredje ledd uttaler departementet at personopplysningsloven § 23 som utgangspunkt ikke gjelder for en arbeidsgivers egen etterforskning, men at det må foretas en konkret vurdering av situasjonen. Departementet

[129] Ot.prp. nr. 92 (1998-1999) side 121.

anser muligheten til å foreta speilkopiering for å sikre bevis, som et element i denne vurderingen.[130] I tillegg vil det i den konkrete vurderingen av om § 23 kommer til anvendelse, være naturlig å vektlegge om arbeidsgiveren foretar innsynet som et ledd i politiets etterforskning. Det kan hevdes at dess nærmere arbeidsgiverens handlinger er knyttet til politiets etterforskning, dess sterkere taler det for at informasjon kan unnlates. Det må imidlertid presiseres at det kun er når hemmelighold er *"påkrevd"* at varslingsplikten kan tilsidesettes, jf. personopplysningsloven § 23 første ledd bokstav b. I de færreste tilfellene vil det være påkrevd å unnlate også etterfølgende varsel etter § 9-3 annet ledd.

5.5.5 Forholdet mellom personopplysningsforskriften § 9-3 og reglene i personopplysningsloven – sett i lys av Norges EØS-rettslige forpliktelser

5.5.5.1 Innledning

Etter bestemmelsen i forskriften § 9-3 kan altså forutgående varsling av innsyn utelates i en del tilfeller. Et interessant spørsmål er hvordan denne regelen forholder seg til reglene om informasjonsplikt i personopplysningsloven.

5.5.5.2 Særlig om forholdet til personopplysningsloven § 19

I henhold til personopplysningsloven § 19 skal det som nevnt gis informasjon før det samles inn personopplysninger fra den registrerte selv.[131] Når det er klart at eksempelvis e-postmeldinger regnes som personopplysninger, er det betimelig å spørre om ikke regelen i § 19 innebærer at det *alltid* skal varsles *før* innsyn foretas.

For det første må det avgjøres om § 19 i det hele tatt kommer til anvendelse ved innsyn i e-post og elektronisk utstyr, som kontrolltiltak i arbeidslivet. Dersom dette er tilfelle må det avgjøres om det foreligger en konflikt mellom reglene i forskriften § 9-3 og

[130] FADs merknader side 4.
[131] Se punkt 3.3.2.

personopplysningsloven § 19. Ved eventuell motstrid må det tas stilling til hvilken regel som gjelder.

For at § 19 skal komme til anvendelse, må innsyn i e-post og annet elektronisk utstyr regnes som innsamling av opplysninger *"fra den registrerte selv"*. Ordlyden kan indikere at det kreves en viss direkte kontakt mellom arbeidsgiveren og arbeidstakeren. Dette vil ikke være tilfelle ved innsyn. Det uttales imidlertid i forarbeidene at ikke bare direkte oppfordringer om å gi informasjon rammes. Også mer indirekte innsamling omfattes, for eksempel der den registrerte etterlater seg elektroniske spor. Innsamlingen må imidlertid bunne ut i et ønske om å tilegne seg informasjon om vedkommende.[132] Dette vil ofte gjelde ved innsyn, og slike kontrolltiltak vil dermed kunne hevdes å være underlagt informasjonsplikten i § 19.

Også reelle hensyn taler for at § 19 kommer til anvendelse. Det kan synes unaturlig at det gjelder en informasjonsplikt dersom arbeidstakeren fysisk anmodes om å overgi informasjon, mens informasjonsplikten kan omgås ved å tilegne seg opplysningene på en mer fordekt måte.

I merknadene til forskriften § 9-3 er ikke forholdet til § 19 nevnt. Det foreligger heller ikke rettspraksis der § 19 har vært avgjørende for at en varslingsplikt før e-postinnsyn kunne statueres. Datatilsynet har imidlertid i sin praksis ansett det klart at informasjonsplikten i § 19 gjelder ved innsyn i ansattes e-post. I en sak uttalte tilsynet at man i slike tilfeller ikke en gang beveger seg i lovens grenseområde.[133]

I forbindelse med en sak der Datatilsynet hadde anmeldt en arbeidsgiver til politiet for brudd på personopplysningsloven, uttalte Riksadvokaten seg om betydningen av § 19 ved innsyn i ansattes e-post.[134] Etter Riksadvokatens oppfatning er ikke slikt innsyn omfattet av informasjonsplikten i § 19. Det er ikke naturlig å si at det å gå gjennom opplysninger om

[132] Ot.prp. nr. 92 (1998-1999) side 119.
[133] Sak 2005/1193 *Datatilsynet−Bazar forlag* dok. 23 side 12.

den registrerte på virksomhetens egen server, er å samle inn opplysninger *"fra den registrerte selv"*. Riksadvokatens argumentasjon er ikke umiddelbart overbevisende, sett i lys av uttalelsene i forarbeidene til § 19 om at også indirekte innsamling av elektroniske spor omfattes av bestemmelsen.

Riksadvokaten fremhever videre at det ville vært naturlig, dersom loven skulle ramme slike forhold, at spørsmålet var nevnt i forarbeidene. Da forarbeidene ble utarbeidet på slutten av 1990-tallet, var det jo ikke uvanlig å bruke e-post i mange virksomheter. Heller ikke dette argumentet er særlig overbevisende. At innsyn i arbeidstakeres e-post var et sentralt tema på dette tidspunktet synes tvilsomt. Dette underbygges av at det øyensynlig ikke finnes noe rettspraksis der problemstillingen behandles fra før 2000. Mot Riksadvokatens syn kan det videre innvendes at reglene i personopplysningsloven er svært generelt utformet og er ment å ha et stort anvendelsesområde. Det ville være en vanskelig oppgave for lovgiver å skildre alle tilfeller der reglene kommer til anvendelse. At spørsmålet ikke er nevnt i forarbeidene synes altså ikke avgjørende for at § 19 ikke kommer til anvendelse ved innsyn i e-post.

Det kan tale mot at regelen kommer til anvendelse at noe av formålet med informasjonsplikten i § 19 er at den registrerte skal få nok informasjon til å avgjøre om vedkommende ønsker å gi fra seg opplysningene.[135] Der en arbeidsgiver i henhold til forskriften § 9-2 har innsynsrett, er det ikke avgjørende om arbeidstakeren frivillig vil gi fra seg opplysningene. Dette kan hevdes å tale mot at bestemmelsen i § 19 gjelder ved innsyn i e-post.

Dette motargumentet kan likevel ikke være avgjørende. Bestemmelsen i § 19 er etter sin ordlyd forutsatt å gjelde også i tilfeller der innsamlingen ikke skjer frivillig, jf. § 19 første ledd bokstav d. Sett i sammenheng med forarbeidene til bestemmelsen og Datatilsynets praksis, synes det riktig å legge til grunn at personopplysningsloven § 19 i utgangspunktet kommer til anvendelse ved innsyn i e-post og annet elektronisk utstyr.

---

[134] Sak 2005/1003 *Datatilsynet–Vinmonopolet AS* dok. 29.
[135] Ot.prp. nr. 92 (1998-1999) side 119.

Det neste spørsmålet er om § 19 likevel skal tilsidesettes etter innføringen av de nye særbestemmelsene om innsyn i personopplysningsforskriften kapittel 9. Som nevnt innebærer § 19 at det må gis informasjon *før* innsamling av personopplysninger gjennomføres. I henhold til forskriften § 9-3 kan varsel i gitte situasjoner gis *etter* at innsynet er gjennomført.

Det er ikke opplagt at det foreligger noe motsetningsforhold mellom de to reglene. Trolig innebærer § 19 bare en regel om at informasjon må gis på ett eller annet tidspunkt før innsynet, gjerne på ansettelsestidspunktet,[136] mens § 9-3 regulerer varslingsplikten i forbindelse med det konkrete kontrolltiltaket. Imidlertid er det lite som tyder på at lovgiver har tenkt forskriften supplert av § 19. Ordlyden i § 9-3 gir ikke inntrykk av at det er forutsatt alltid å gjelde en informasjonsplikt før innsyn. Spørsmålet kan altså stilles, om forskriftens bestemmelser i henhold til prinsippene om lex posterior og lex specialis medfører at personopplysningsloven § 19 må tilsidesettes.

For å underbygge forskriftens selvstendige stilling, synes det nærliggende å vise til arbeidsmiljøloven § 9-5. Her heter det at arbeidsgivers rett til innsyn i arbeidstakers e-post reguleres av personopplysningsforskriften. Det vises altså kun til forskriften, ikke til personopplysningsloven. I forarbeidene til arbeidsmiljøloven § 9-5 uttales det imidlertid at hensikten med bestemmelsen var å gjøre oppmerksom på at innsyn i e-post og elektronisk utstyr bare kan skje når det følger av *"personopplysningslovens regler"*.[137] At det vises direkte vil forskriftens regler i den formelle lovregelen i arbeidsmiljøloven § 9-5, kan altså ikke være avgjørende for at ikke personopplysningslovens regler kommer til anvendelse ved innsyn i e-post.

Som nevnt bygger personopplysningsloven § 19 på EUs personverndirektiv art. 10. Det taler åpenbart mot at § 19 skal tilsidesettes, dersom dette innebærer et brudd på Norges

[136] Se punkt 3.3.2.
[137] Ot.prp. nr. 71 (2007-2008) side 5.

EØS-rettslige forpliktelser. Det må altså avgjøres om Norge i henhold til EU-direktivet plikter å ha regler som pålegger en informasjonsplikt *før* det foretas innsyn.

Det er naturlig å først ta stilling til om informasjonsplikten i art. 10 i det hele tatt gjelder ved innsyn i en arbeidstakers e-post eller elektroniske utstyr. Selv om personopplysningsloven § 19 som nevnt trolig er anvendelig, trenger ikke nødvendigvis art. 10 å være det. Ved vurderingen av om § 19 kommer til anvendelse er jo som nevnt de norske lovforarbeidene en tungtveiende rettskildefaktor. Det kan dessuten igjen nevnes at EU-direktivet er et minimumsdirektiv, og at § 19 av den grunn kan oppstille en strengere informasjonsplikt enn direktivet legger opp til. [138]

Ordlyden i art. 10 synes etter en naturlig fortolkning å tale mot at bestemmelsen gjelder ved innsyn. Den taler i enda større grad enn personopplysningsloven § 19 for at det kreves en direkte kontakt mellom den registrerte og den behandlingsansvarlige. Det heter blant annet at det skal gis informasjon om hvorvidt *"replies to the questions"* er frivillige eller ikke. Bestemmelsen synes altså å forutsette at innsamlingen av opplysninger skjer ved spørsmål og svar. På den annen side kan hensynet til å unngå omgåelser av bestemmelsen tale for at informasjonsplikten i art. 10 også må gjelde ved indirekte innsamling. Dette hensynet fremheves i direktivets fortale.[139] Spørsmålet om art. 10 gjelder ved innsyn i e-post er øyensynlig ikke behandlet av EF-domstolen. Slik jeg ser det, er det nokså uklart om art. 10 inneholder en forpliktelse for Norge til å oppstille en informasjonsplikt ved innsyn i e-post.

Det er likevel ikke gitt at det er nødvendig å besvare dette spørsmålet. Det følger av EU-direktivet art. 10 at det bare skal gis informasjon *"in cases of collection of data from the data subject"*. Det oppstilles altså ikke etter ordlyden noe eksplisitt krav om at informasjonen gis *før* innsamlingen. Dermed kan det hevdes at forpliktelsen i art. 10, forutsatt at den kommer til anvendelse, er oppfylt gjennom varslingsregelen i forskriften

[138] Se punkt 2.2.7.
[139] Se fortalen avsnitt 27.

§ 9-3, og at § 9-3 i henhold til EØS-retten alene kan regulere arbeidsgivers informasjonsplikt ved innsyn i de ansattes e-post og elektroniske utstyr.

Selv om spørsmålet ikke er helt avklart er det etter dette nærliggende å anta at varslingsplikten i forskriften § 9-3 ikke suppleres av en plikt etter personopplysningsloven § 19 til alltid å måtte gi informasjon *før* innsyn.

5.5.5.3 Særlig om forholdet til personopplysningsloven § 20

Personverndirektivet art. 11 inneholder en regel om informasjonsplikt i tilfeller der personopplysninger innhentes fra andre kilder enn den registrerte selv. Etter forarbeidene til personopplysningsloven er art. 11 implementert i norsk rett gjennom bestemmelsen i personopplysningsloven § 20.[140] I henhold til § 20 skal det informeres når personopplysninger samles inn fra *"andre"* enn den registrerte selv. Det synes altså forutsatt at informasjonen innhentes fra en tredjeperson. Dette vil ikke være tilfelle ved innsyn i arbeidstakeres e-postkasse eller PC. Ordlyden i § 20 trekker i retning av at bestemmelsen ikke kommer til anvendelse ved slikt innsyn.

Art. 11 er imidlertid utformet på en annen måte. Etter direktivbestemmelsen må det informeres i tilfeller *"where the data have not been obtained from the data subject"*. Etter ordlyden forutsettes det altså ikke at informasjonen nødvendigvis er innhentet fra noen fysisk tredjeperson. Art. 11 kan etter dette synes å oppstille en informasjonsplikt ved innsyn i e-post. Tolket i lys av direktivbestemmelsen vil personopplysningsloven § 20 måtte komme til anvendelse ved slikt innsyn. Videre nevnes at det finnes tilfeller fra Datatilsynets praksis der informasjonsplikt ved innsyn i e-post ble hjemlet i personopplysningsloven §§ 19 og 20 uten at tilsynet spesifiserte hvilken av de to bestemmelsene tilsynet anså overtrådt.[141]

---

[140] Ot.prp. nr. 92 (1998-1999) side 119.
[141] Se for eksempel sak 2005/1003 *Datatilsynet – Vinmonopolet AS.*

I henhold til § 20 skal informasjon gis *"så snart opplysningene er innhentet"*. Etter ordlyden kreves det altså ikke at det er informert *før* innsyn er foretatt. I henhold til art. 11 skal det informeres *"at the time of undertaking the recording of personal data"*. Med dette siktes det tilsynelatende til tidspunktet for lagringen av opplysningene, *etter* at innsynet er gjennomført. Det følger av personopplysningsforskriften § 9-3 at det så langt mulig skal varsles i forkant av innsynet, og dersom dette ikke er gjort, må det varsles så snart innsynet er gjennomført. I relasjon til art. 11 må det etter dette antas at forskriften § 9-3 oppfyller den EØS-rettslige forpliktelsen.

5.5.5.4 Generelt

At varsling i enkelte tilfeller kan foretas *etter* at innsynet er gjennomført, innebærer altså trolig ikke noe brudd på Norges EØS-rettslige forpliktelser. Imidlertid statuerer art. 10 og art. 11 tilsynelatende en noe mer omfattende informasjonsplikt rent *innholdsmessig* enn bestemmelsen i § 9-3. Særlig bør det nevnes at den registrerte i henhold til direktivbestemmelsene skal gis informasjon om sin rett til innsyn i de innsamlede personopplysningene.[142] Forutsatt at en av direktivbestemmelsene regulerer informasjonsplikt ved innsyn i e-post, må listen over opplysninger oppstilt i § 9-3 suppleres med informasjon om innsynsretten som følger av personopplysningsloven § 18.[143] I motsatt fall foreligger trolig et brudd på Norges EØS-rettslige forpliktelser.

[142] Dette følger av direktivet art. 12, som er implementert gjennom personopplysningsloven § 18.
[143] Se punkt 3.3.2.

6 Kilderegister

6.1 Litteratur

Bruun, Hilde Foyn
Forarbeider til forskrifter. Noen rettskildeteoretiske og forvaltningsrettslige aspekter
Stensilserie (Universitetet i Oslo, Institutt for offentlig rett)
Bind 34, 1980

Dege, Jan Tormod
Arbeidsgivers styringsrett bind 1 Ytre rammevilkår og arbeidsavtalen
Minerva, 1995

Eckhoff, Torstein
Rettskildelære
5. utgave ved Jan E. Helgesen
Universitetsforlaget, 2000

Fanebust, Arne
Innføring i arbeidsrett
2. utgave
Universitetsforlaget, 2002

Jakhelln, Henning og Aune, Helga
Arbeidsrett.no Kommentar til arbeidsmiljøloven
N.W. Damm og Søn, 2005

Jakhelln, Henning
Oversikt over arbeidsretten
4. utgave
N.W. Damm og Søn, 2006

Melsom, Nina
Hvilken rett har arbeidsgiver til å gjøre seg kjent med arbeidstakernes e-post?
Arbeidsrett, 2004 nr. 3 side 178-185

6.2 Lover og forskrifter

Norske lover

Lov om mekling og rettergang i sivile tvister av 17. juni 2005 nr. 90 (tvisteloven)

Lov om arbeidsmiljø, arbeidstid og stillingsvern mv. av 17. juni 2005 nr. 62 (arbeidsmiljøloven)

Lov om behandling av personopplysninger av 14. april 2000 nr. 31 (personopplysningsloven)

Lov om styrking av menneskerettighetenes stilling i norsk rett av 21. mai 1999 nr. 30 (menneskerettsloven)

Lov om gjennomføring i norsk rett av hoveddelen i avtale om Det europeiske økonomiske samarbeidsområde (EØS) m.v. av 27. november 1992 nr. 109 (EØS-loven)

Lov om personregistre mm. av 9. juni 1978 nr. 48 (personregisterloven) (opphevet)

Almindelig borgerlig Straffelov av 22. mai 1902 nr. 10 (straffeloven)

Norske forskrifter

Forskrift om behandling av personopplysninger av 15. desember 2000 nr. 1265 (personopplysningsforskriften)

Utenlandske lover

Lag om integritetsskydd i arbetslivet av 13.august 2004 nr. 759 (finsk)

6.3 Forarbeider

Norges offentlige utredninger

NOU 2009: 1 *Individ og integritet Personvern i det digitale samfunnet*

NOU 2004: 5 *Arbeidslivslovutvalget Et arbeidsliv for trygghet, inkludering og vekst*

NOU 1997: 19 *Et bedre personvern - forslag til lov om behandling av personopplysninger*

Odelstingsproposisjoner

Ot.prp. nr. 71 (2007-2008) *Om lov om endringer i personopplysningsloven mv. (forskriftshjemmel, overtredelsesgebyr og innkreving av tvangsmulkt)*

Ot.prp. nr. 49 (2004-2005) *Om lov om arbeidsmiljø, arbeidstid og stillingsvern mv. (arbeidsmiljøloven)*

Ot.prp. nr. 92 (1998-1999) *Om lov om behandling av personopplysninger (personopplysningsloven)*

Ot.prp. nr. 56 (1992-1993) *Om lov om endringer i lov 9 juni 1978 nr 48 om personregistre m.m (fjernsynsovervåkning)*

Ot.prp. nr. 56 (1989-1990) *Om lov om megling i konfliktråd og om endringer i straffeloven m.m. (hemmelig opptak av samtale og offentlig gjengivelse; fjernsynsovervåkning; uforsiktig omgang med skytevåpen; ulovlig innførsel, produksjon og omsetning av alkohol; falsk utrykningsmelding; skyldkravet ved heleri m.m.)*

Forarbeider til forskrifter

Merknader til personopplysningsforskriften kapittel 9
Fornyings- og administrasjonsdepartementet
1. mars 2009
http://www.regjeringen.no/nb/dep/fad/aktuelt/nyheter/2009/fra-i-dag-gjelder-de-nye-reglene-for-inn.html?id=547499

Til personopplysningsforskriften
Justis- og politidepartementet
15. desember 2000
http://www.regjeringen.no/nb/dep/jd/dok/lover_regler/reglement/2000/Forskrift-til-personopplysningsloven-personopplysningsforskriften/2.html?id=278534.

Delegering av Kongen sin forskriftskompetanse etter personopplysningsloven til Fornyings- og administrasjonsdepartementet
Kongelig resolusjon nr. 345
11. april 2008

Høringsbrev

Forslag til regler om arbeidsgivers adgang til ansattes e-post mv.
Endring av personopplysningsloven, nytt kapittel i personopplysningsforskriften og ny bestemmelse i arbeidsmiljøloven med vedlagt høringsnotatet *Forslag til regler om arbeidsgivers tilgang til ansattes e-post mv.*
Fornyings- og administrasjonsdepartementet
17. oktober 2006
http://www.regjeringen.no/nb/dep/fad/dok/Horinger/Horingsdokumenter/2006/forslag-til-regler-om-arbeidsgivers-adga/1.html?id=270943.

6.4 Norsk rettspraksis

Norsk Retstidende

Rt. 2005 side 518

Rt. 2004 side 878

Rt. 2002 side 1572

Rt. 2002 side 1500

Rt. 2001 side 1589 (Raufoss)

Rt. 2001 side 668 (Tippekassekjennelsen)

Rt. 2001 side 418 (Kårstø)

Rt. 2000 side 1602 (Nøkk)

Rt. 2000 side 996 (Bøhler)

Rt. 1997 side 786

Rt. 1991 side 616 (Gatekjøkkenkjennelsen)

Rt. 1974 side 1089

Rettens Gang

RG 2004 side 347 (Borgarting lagmannsrett)

RG 2004 side 198 (Oslo tingrett)

RG 2002 side 162 (Gulating lagmannsrett)

Øvrig rettspraksis

26. mai 2008 Borgarting lagmannsrett (LB-2007-121782)

24. april 2002 Oslo tingrett (TOSLO-2001-12516) (Oslo Sporveier)

6.5 Direktiver og internasjonale avtaler

Direktiver

Europaparlaments- og rådsdirektiv 95/46/EF av 24. oktober 1995 om beskyttelse av fysiske personer i forbindelse med behandling av personopplysninger og om fri utveksling av slike opplysninger (personverndirektivet)
Innlemmet i EØS-avtalen ved EØS-komiteens beslutning nr. 83/1999

Internasjonale avtaler

Den Europeiske Menneskerettighetskonvensjon (EMK)
Inkorporert i norsk lovgivning ved menneskerettsloven av 21. mai 1999 nr. 30

Avtale om Det europeiske økonomiske samarbeidsområde (EØS-avtalen)
Inkorporert i norsk lovgivning ved EØS-loven av 27. november 1992 nr. 109

6.6 Praksis fra EMD

03. april 2007 *Copland – Storbritannia*

16. desember 1992 *Niemitz – Tyskland*

6.7 Praksis fra Personvernnemnda og Datatilsynet

Personvernnemnda klagesak 2005 nr. 1
http://www.personvernnemnda.no/vedtak/2005_1.htm

Datatilsynet sak 2005/1193 mot Bazar forlag

Datatilsynet sak 2005/1003 mot Vinmonopolet AS

6.8 Øvrige kilder

Datatilsynet

E-poster og filer

10. mars 2008

http://www.datatilsynet.no/templates/article____201.aspx

Datatilsynet

Når har du lov til å overvåke med kamera?

Juli 2004

http://www.datatilsynet.no/templates/article____401.aspx

Riksadvokaten

Avgjørelse i klagesak over henleggelse

Vedlagt brev til Datatilsynet av 26. mars 2007

Lagret hos Datatilsynet som sak 2005/1003 dokument 29

A